

Kyle McLean, Esq. (SBN #330580)
 Email: kmclean@sirillp.com
 Mason Barney, Esq. (*Pro Hac Vice*)
 Email: mbarney@sirillp.com
 Tyler Bean, Esq. (*Pro Hac Vice*)
 Email: tbean@sirillp.com
 SIRI & GLIMSTAD LLP
 700 S. Flower Street, Ste. 1000
 Los Angeles, CA 90017
 Telephone: 213-376-3739

Interim Class Counsel

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

In re

DATA BREACH SECURITY LITIGATION
AGAINST BRIGHTLINE, INC.

No. C 23-02132 WHA
 No. C 23-02291 WHA
 No. C 23-02503 WHA
 No. C 23-02909 WHA

(Consolidated)

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Terrance Rosa, Ryan Watson, Donisha Jackson, Kyle Castro, on behalf of
 himself and his minor children, E.N.C., C.J.C., and E.J.C., Itaunya Milner, on behalf of herself and
 her minor child, B.G., and Anthony Ndifor, on behalf of themselves, and on behalf of all similarly
 situated persons, allege the following against Brightline, Inc. ("Brightline" or "Defendant") based
 upon personal knowledge with respect to themselves and on information and belief derived from,
 among other things, investigation by their counsel and review of public documents as to all other
 matters:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard Plaintiffs’ and other similarly situated individuals’ (defined herein as “Class Members”) personally identifiable information (“PII”) and protected health information (“PHI”), including individuals’ names, addresses, dates of birth, member identification numbers, start and end dates of health plan coverage, Social Security numbers, and/or employer names (the “Private Information”),¹ from unauthorized disclosure to cybercriminals.

2. Defendant Brightline is a mental and behavioral health provider offering virtual counseling for children, teenagers, and their families. It is based in San Mateo, California. Brightline maintains the PII and PHI of its direct patients and its business clients’ employees and their children, including that of Plaintiffs and Class Members.

3. Despite having duties created by statute and common law to safeguard that Private Information entrusted to it, Brightline allowed this PII and PHI, including PII and PHI belonging to minor children, to be stolen and then posted on the dark web by a notorious cybercriminal organization calling itself Cllop.

4. On or about January 30, 2023 or earlier, an unauthorized third party or person accessed and downloaded Plaintiffs’ and Class Members’ Private Information. Brightline’s information then appeared on Cllop’s ransomware portal in March 2023.

5. In May 2023, months after it learned about the breach, the company announced the breached publicly and sent out notices to effected patients.

6. In a nearly unprecedented event, after public reporting regarding the data breach, and the work that Brightline does with children, Cllop sent a communication to the website “BleepingComputer.com” stating it had deleted Brightline’s data from its data leak site and apologizing for its actions.

¹ See <https://apps.web.maine.gov/online/aevviewer/ME/40/73c3b1aa-9062-47c2-93a1-a728df66f8ee.shtml> (last visited on Sept. 19, 2023).

1 7. Nevertheless, the data was still posted on Clop's data leak website for at least 50
2 days, during which numerous bad actors almost certainly downloaded the data, meaning they could
3 still use the data or re-sell the data to yet more bad actors. Likewise, as the BleepingComptuer.com
4 article states, there is no evidence that Clop fully deleted all the information it had stolen, meaning
5 it could later change its mind and start re-selling the data. Thus, Clop's apparent act of contrition
6 does not mean that Plaintiff and the Class Members' data is now safe from exploitation. But, the
7 fact that an infamous gang like Clop would feel any remorse for stealing children's mental health
8 information shows just how sensitive and dangerous this PII and PHI can be in the wrong hands.

9 8. Plaintiffs bring this class action lawsuit to address Defendant's collective
10 inadequate safeguarding and supervision of Class Members' Private Information that it collected
11 and maintained.

12 9. Defendant has independent, non-delegable duties to its patients and clients'
13 employees to safeguard their PHI and PII and is responsible for the wrongful disclosure of
14 Plaintiffs' and Class Members' Private Information.

15 10. As a result of Brightline's impermissibly lax data security practices, Plaintiffs and
16 Class Members are at a present and continuing risk for identity and medical identity theft.
17 Brightline then compounded this harm by waiting months before notifying affected individuals
18 that their highly sensitive Private Information was now in the hands of sophisticated cyber
19 criminals.

20 11. Defendant failed to comply with industry standards to protect patients' and its
21 clients' employees' Private Information and failed to provide adequate notice to Plaintiffs and
22 other Class Members that their PII and PHI had been compromised.

23 12. Taking reasonable, standard precautions against cybercrime and data breaches is a
24 fundamental duty of doing business in the modern age—especially for businesses like Brightline
25 that profit from analyzing and processing Private Information. By collecting, maintaining, and
26 profiting from Plaintiffs' and Class Members' Private Information, Brightline was required by law
27
28

1 to exercise reasonable care and comply with industry and statutory requirements to protect that
2 information—and it failed to do so.

3 13. Among myriad industry standards and statutes for protection of sensitive
4 information, health care information is specifically governed by federal law under the Health
5 Insurance Portability and Accountability Act of 1996 (“HIPAA”) and its implementing
6 regulations. HIPAA requires entities like Brightline to take appropriate technical, physical, and
7 administrative safeguards to secure the privacy of PHI, establishes national standards to protect
8 PHI, and requires timely notice of a breach of unencrypted PHI.

9 14. Instead, Brightline’s woefully inadequate data security measures made the Data
10 Breach a foreseeable, and even likely, consequence of its negligence. Brightline disregarded the
11 rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing
12 to implement reasonable measures to safeguard its patients’ Private Information and by failing to
13 take necessary steps to prevent unauthorized disclosure of that information. Brightline then further
14 violated its obligations under HIPAA by waiting an unreasonably long time to notify its patients
15 about the Data Breach.

16 15. By aggregating the Private Information obtained from the Data Breach with other
17 sources, or other methods, criminals can assemble a full dossier of Private Information on an
18 individual in order to facilitate a wide variety of frauds, thefts, and scams. Criminals can and do
19 use victims’ names, birth dates, insurance information, Social Security numbers, and addresses to
20 open new financial accounts, incur charges in credit, obtain government benefits and
21 identifications, fabricate identities, and file fraudulent tax returns well before the person whose PII
22 was stolen becomes aware of it.² Any one of these instances of identity theft can have devastating
23

24 ² See, e.g., *Report to Congressional Requesters*, U.S. GOV’T ACCOUNTABILITY OFFICE (June 2007),
25 <http://www.gao.gov/assets/270/262899.pdf>; Melanie Lockert, *How do hackers use your*
26 *information for identity theft?*, CREDITKARMA (Oct. 1, 2021), [https://www.creditkarma.com/id-](https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information)
27 [theft/i/how-hackers-use-your-information](https://www.creditkarma.com/id-theft/i/how-hackers-use-your-information); Ravi Sen, *Here’s how much your Private Information*
28 *is worth to cybercriminals—and what they do with it*, PBS (May 14, 2020),
[https://www.pbs.org/newshour/science/ heres-how-much-your-personal-information-is-worth-to-](https://www.pbs.org/newshour/science/heres-how-much-your-personal-information-is-worth-to-)

consequences for the victim, causing years of often irreversible damage to their credit scores, financial stability, and personal security.

16. Likewise, the exfiltration of PHI puts Plaintiffs and Class Members at a present and continuing risk for medical identity theft, especially in light of the high demand and value of Medicare identification numbers on the dark web.³ Medical identity theft poses an even more critical threat to victims—medical fraud could lead to loss of access to necessary healthcare through misuse of paid-for insurance benefits or by incurring substantial medical debt.

17. Due to the highly valuable nature of PHI, the FBI has warned healthcare providers that they are likely to be the targets of cyberattacks like the attack that caused the Data Breach.⁴

18. Adding insult to injury, there has been no assurance offered by Brightline that all personal data or copies of data have been recovered or destroyed, or that Brightline has adequately enhanced its security practices or dedicated sufficient resources and staff and to avoid a similar breach of its network in the future.

19. As a direct and proximate result of the Data Breach, Plaintiffs and Class Members have suffered actual and present injuries, including but not limited to, present and continuing threats of identity theft crimes, fraud, scams, and other misuses of their Private Information; ongoing monetary loss and economic harm, including loss of value of their Private Information; loss of value of privacy and confidentiality of the stolen Private Information; illegal sales of the compromised Private Information; mitigation expenses and time spent on credit monitoring; identity theft insurance costs; credit freezes/unfreezes; expense and time spent on initiating fraud alerts and contacting third parties; decreased credit scores; lost work time; and other injuries.

cybercriminals-and-what-they-do-with-it; Alison Grace Johansen, *4 Lasting Effects of Identity Theft*, LIFELOCK BY NORTON (Feb. 4, 2021), <https://lifelock.norton.com/learn/identity-theft-resources/lasting-effects-of-identity-theft>.

³ *What to Know About Medical Identity Theft*, FED. TRADE COMM'N (May 2021), <https://consumer.ftc.gov/articles/what-know-about-medical-identity-theft>.

⁴ Jim Finkle, *FBI warns healthcare firms they are targeted by hackers*, REUTERS (Aug. 20, 2014), <https://www.reuters.com/article/us-cybersecurity-healthcare-fbi-idUSKBN0GK24U20140820>.

20. Plaintiffs and Class Members would not have provided their valuable PII and sensitive PHI to their respective health plans or other entities to in turn provide that information to Brightline had they known that Brightline would make the Private Information internet-accessible, not encrypt personal and sensitive data elements, and not delete the Private Information it no longer had reason to maintain.

21. Through this lawsuit, Plaintiffs seek to hold Brightline responsible for the injuries it inflicted on Plaintiffs and nearly 1,000,000 similarly situated individuals, including children, due to its impermissibly inadequate data security measures, and to seek injunctive relief to ensure the implementation of security measures to protect the Private Information which remains in the possession of Brightline.

II. PARTIES

22. Plaintiff Terrance Rosa is, and at all times mentioned herein was, an individual citizen of Pennsylvania.

23. Plaintiff Ryan Watson is, and at all times mentioned herein was, an individual citizen of Virginia.

24. Plaintiff Donisha Jackson is, and at all times mentioned herein was, an individual citizen of Illinois.

25. Plaintiff Kyle Castro is, and at all times mentioned herein was, an individual citizen of Tennessee.

26. Itaunya Milner is, and at all times mentioned herein was, an individual citizen of New Jersey.

27. Plaintiff Anthony Ndifor is, and at all times mentioned herein was, an individual citizen of California.

28. Defendant Brightline, Inc. is a Delaware corporation, with its principal place of business in San Mateo, California.

III. JURISDICTION AND VENUE

29. This Court has original jurisdiction under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because this is a class action involving more than 100 putative Class Members and the amount in controversy exceeds \$5,000,000, exclusive of interest and costs. Minimal diversity is established because Plaintiffs (and many members of the Class) are citizens of states different than Brightline.

30. This Court has general personal jurisdiction over Brightline because Brightline's principal place of business and headquarters is in this District. Brightline also regularly conducts substantial business in this District.

31. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) because a substantial part of the events giving rise to the claims emanated from activities within this District, and Brightline conducts substantial business in this District.

IV. FACTUAL ALLEGATIONS

A. Defendant's Business and Collection of Plaintiffs' and Class Members' Private Information

32. Founded in 2019, Brightline, Inc. provides mental and behavioral health services, including virtual counseling for children, teenagers and their families and is based in San Mateo, California.

33. Upon information and belief, Brightline employs more than 140 people and generates approximately \$20 million in annual revenue, but reportedly has received over \$200 million in venture capital funding.

34. As a condition for receiving pediatric behavioral health and/or benefit eligibility, Class members were required by Brightline to confide and make available to it, its agents, and its employees, sensitive and confidential PII and PHI.

35. In its Notice of HIPAA Privacy Practices (referred to herein as the "Privacy Policy"), Brightline makes it clear that "[t]he protection of [its patients'] health information is very

important” to it, and that it will only release this protected information “with your permission, or under circumstances,” none of which listed circumstances are applicable here.⁵

36. By obtaining, collecting, using, and deriving a benefit from Plaintiffs’ and Class Members’ Private Information, Defendant assumed legal and equitable duties owed to them and knew or should have known that it was responsible for protecting Plaintiffs’ and Class Members’ Private Information from unauthorized disclosure and exfiltration.

37. Plaintiffs and Class Members relied on Defendant to keep their Private Information confidential and securely maintained and to only make authorized disclosures of this Information, which Defendant ultimately failed to do.

B. The Data Breach

38. Fortra was one of Defendant’s “business associates.” Nevertheless, on February 1, 2023, cybersecurity expert Brian Krebs reported that Fortra disclosed to its customers a “remote code injection exploit” affecting GoAnywhere MFT, Fortra’s widely used file transfer application. Hackers used “remote code injection exploits” to remotely execute malicious code on their targets’ computer systems.

39. On or around February 10, 2023, the Russia-linked ransomware group, Cl0p, claimed to be responsible for attacks on GoAnywhere MFT and to have stolen data exposed by the software from over 130 organizations over the course of the preceding ten days. Brightline Inc. was listed as one of those organizations.

40. On or about May 5, 2023, three months after learning of the Data Breach, Brightline publicly announced through its website⁶ that it was one of the entities impacted, and that the PII and PHI of certain of its patients and employees of its clients were exposed.

⁵ See <https://www.hellobrightline.com/privacy-practices> (last visited on Sept. 19, 2023).

⁶ <https://www.hellobrightline.com/fortra-data-notice>

41. Through the Data Breach, the unauthorized cybercriminals accessed a cache of highly sensitive Private Information, including medical records, Social Security numbers, past and current medications and health insurance information.

42. Defendant delivered its Notice to Plaintiffs and Class Members between mid-April and mid-May 2023, over three months after learning of the Data Breach, alerting them that their highly sensitive Private Information had been exposed. The initial notices sent in April 2023 were just sent to approximately 28,000 effected patients. The over 900,000 other effected patients were not notified until May 2023.

43. Following this announcement, the Data Breach received widespread coverage in the media. One of the outlets that covered it was the website BleepingComputers.com, a website known for its reporting on data breaches. The website stated that at the time of the article the Brightline data breach was thought to impact 783,606 patients, “[h]owever, this figure may increase as internal investigations progress.”⁷ In addition to reporting on the notice issued by the company, BleepingComputer.com also reported that: “Brightline was listed on Clop’s extortion portal on March 16th, 2023, indicating that the health startup was among the firms the ransomware actors breached in their large-scale attack.” The outlet then noted that: “Brightline’s extensive partnerships with healthcare institutes and companies in the U.S. has resulted in a security incident impacting many entities. This includes well-known organizations like Diageo, Nintendo of America Inc., Harvard University, Stanford University, and Boston Children’s Hospital.” Brightline maintains a list of the 64 impacted entities on its website: <https://www.hellobrightline.com/list-of-impacted-covered-entities>.

44. After BleepingComputer.com posted its news story on May 3, 2023, the Clop ransomware gang emailed the website on May 5, 2023 to state that it removed Brightline’s information from its data leak website. The gang told BleepingComputer.com that:

⁷ <https://www.bleepingcomputer.com/news/security/brightline-data-breach-impacts-783k-pediatric-mental-health-patients/#:~:text=Update%205%2F3%2F23%3A,not%20all%20companies%20are%20analyzing>

1 We delete the data and we did not know what this company is doing,
 2 because not all companies are analyzing. And we ask for forgiveness
 3 for this incident.⁸

4 45. BleepingComputer.com was unable to confirm whether Clop had fully deleted the
 5 information in its possession, but the website did confirm that Brightline was no longer listed on
 6 the gang's data leak website. BleepingComputer.com also provided no information regarding who
 7 had downloaded the Brightline files from Clop's data link website in the 50 days between March
 8 16th and May 5th.

9 46. Defendant had obligations created by contract, industry standards, common law,
 10 federal and state regulations, and representations made to Plaintiffs and Class Members to keep
 11 Plaintiffs' and Class Members' Private Information confidential and to protect it from
 12 unauthorized access and disclosure.

13 47. Plaintiffs and Class Members provided their Private Information to Defendant with
 14 the reasonable expectation and mutual understanding that Defendant would comply with its
 15 obligations to keep such Information confidential and secure from unauthorized access.

16 48. Defendant's data security obligations were particularly important given the
 17 substantial increase in cyberattacks in recent years.

18 49. Defendant knew or should have known that its electronic records would be targeted
 19 by cybercriminals.

20 **C. The Healthcare Sector is Particularly Susceptible to Data Breaches**

21 50. Defendant was on notice that companies in the healthcare industry are susceptible
 22 targets for data breaches.

23 51. Defendant was also on notice that the FBI has been concerned about data security
 24 in the healthcare industry. In August 2014, after a cyberattack on Community Health Systems,
 25 Inc., the FBI warned companies within the healthcare industry that hackers were targeting them.

26
 27 ⁸ *Id.*
 28

1 The warning stated that “[t]he FBI has observed malicious actors targeting healthcare related
 2 systems, perhaps for the purpose of obtaining the Protected Healthcare Information (PHI) and/or
 3 Personally Identifiable Information (PII).”⁹

4 52. The American Medical Association (“AMA”) has also warned healthcare
 5 companies about the importance of protecting confidential medical information:

6 Cybersecurity is not just a technical issue; it’s a patient
 7 safety issue. AMA research has revealed that 83% of
 8 physicians work in a practice that has experienced some kind
 9 of cyberattack. Unfortunately, practices are learning that
 10 cyberattacks not only threaten the privacy and security of
 11 patients’ health and financial information, but also patient
 12 access to care.¹⁰

13 53. The healthcare sector reported the second largest number of data breaches among
 14 all measured sectors in 2018, with the highest rate of exposure per breach.¹¹ In 2022, the largest
 15 growth in data compromises occurred in the healthcare sector.¹²

18 ⁹ Jim Finkle, *FBI Warns Healthcare Firms that they are Targeted by Hackers*, Reuters (Aug.
 19 2014), available at [https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-](https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820)
 20 [healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820](https://www.reuters.com/article/us-cybersecurity-healthcare-fbi/fbi-warns-healthcare-firms-they-are-targeted-by-hackers-idUSKBN0GK24U20140820) (last visited on Sept.
 19, 2023).

21 ¹⁰ Andis Robeznieks, *Cybersecurity: Ransomware attacks shut down clinics, hospitals*, Am. Med.
 22 Ass’n. (Oct. 4, 2019), available at: [https://www.ama-assn.org/practice-](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals)
 23 [management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals](https://www.ama-assn.org/practice-management/sustainability/cybersecurity-ransomware-attacks-shut-down-clinics-hospitals) (last
 visited on Sept. 19, 2023).

24 ¹¹ Identity Theft Resource Center, *2018 End-of-Year Data Breach Report*, available at:
<https://www.idtheftcenter.org/2018-data-breaches/> (last visited on Sept. 19, 2023).

25 ¹² Identity Theft Resource Center, *2022 End-of-Year Data Breach Report*, available at:
 26 [https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC-2022-Data-Breach-](https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC-2022-Data-Breach-Report-Final-1.pdf)
 27 [Report-Final-1.pdf](https://www.idtheftcenter.org/wp-content/uploads/2023/01/ITRC-2022-Data-Breach-Report-Final-1.pdf) (last visited on Sept. 19, 2023).

54. Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident ... came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.¹³

55. Almost 50 percent of the victims lost their healthcare coverage as a result of the incident, while nearly 30 percent said their insurance premiums went up after the event. Forty percent of the customers were never able to resolve their identity theft at all. Data breaches and identity theft have a crippling effect on individuals and detrimentally impact the economy as a whole.¹⁴

56. Healthcare related breaches have continued to rapidly increase because electronic patient data is seen as a valuable asset. Healthcare providers, like hospitals, “have emerged as a primary target because they sit on a gold mine of sensitive personally identifiable information for thousands of patients at any given time. From social security and insurance policies, to next of kin and credit cards, no other organization, including credit bureaus, have so much monetizable information stored in their data centers.”¹⁵

57. Defendant knew, or should have known, the importance of safeguarding its patients’ Private Information, including PHI, entrusted to it, and of the foreseeable consequences if such data were to be disclosed. These consequences include the significant costs that would be

¹³ Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (March 3, 2010), available at: <https://www.cnet.com/news/privacy/study-medical-identity-theft-is-costly-for-victims/> (last visited on Sept. 19, 2023).

¹⁴ *Id.*

¹⁵ Inside Digital Health, *How to Safeguard Hospital Data from Email Spoofing Attacks*, April 4, 2019, available at: <https://www.chiefhealthcareexecutive.com/view/how-to-safeguard-hospital-data-from-email-spoofing-attacks> (last visited on Sept. 19, 2023).

1 imposed on its patients as a result of a breach. Defendant failed, however, to take adequate
2 cybersecurity measures to prevent the Data Breach from occurring.

3 **D. Defendant Failed to Comply with HIPAA**

4 58. Title II of HIPAA contains what are known as the Administration Simplification
5 provisions. *See* 42 U.S.C. §§ 1301, *et seq.* These provisions require that the Department of Health
6 and Human Services (“HHS”) create rules to streamline the standards for handling PHI similar to
7 the data Defendant left unguarded and vulnerable to attack. The HHS has subsequently
8 promulgated five rules under authority of the Administrative Simplification provisions of HIPAA.

9 59. The Data Breach resulted from a combination of insufficiencies that indicate
10 Defendant failed to comply with safeguards mandated by HIPAA regulations and industry
11 standards. First, it can be inferred from the Data Breach that Defendant either failed to implement,
12 or inadequately implemented, information security policies or procedures to protect Plaintiffs’ and
13 Class Members’ PHI.

14 60. Plaintiffs’ and Class Members’ Private Information compromised in the Data
15 Breach included “protected health information” as defined by CFR § 160.103.

16 61. 45 CFR § 164.402 defines “breach” as “the acquisition, access, use, or disclosure
17 of protected health information in a manner not permitted under subpart E of this part which
18 compromises the security or privacy of the protected health information.”

19 62. 45 CFR § 164.402 defines “unsecured protected health information” as “protected
20 health information that is not rendered unusable, unreadable, or indecipherable to unauthorized
21 persons through the use of a technology or methodology specified by the [HHS] Secretary[.]”

22 63. Plaintiffs’ and Class Members’ Private Information included “unsecured protected
23 health information” as defined by 45 CFR § 164.402.

24 64. Plaintiffs’ and Class Members’ unsecured PHI was acquired, accessed, used, and/or
25 disclosed in a manner not permitted under 45 CFR, Subpart E, as a result of the Data Breach.

26 65. Based upon Brightline’s Notice to Plaintiffs and Class Members, Defendant
27 reasonably believe that Plaintiffs’ and Class Members’ unsecured PHI has been acquired,
28

1 accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E, as a result
2 of the Data Breach.

3 66. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used,
4 and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach
5 was not rendered unusable, unreadable, or indecipherable to unauthorized persons.

6 67. Defendant reasonably believed that Plaintiffs' and Class Members' unsecured PHI
7 that was acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR,
8 Subpart E as a result of the Data Breach was not rendered unusable, unreadable, or indecipherable
9 to unauthorized persons.

10 68. Plaintiffs' and Class Members' unsecured PHI that was acquired, accessed, used,
11 and/or disclosed in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach,
12 and which was not rendered unusable, unreadable, or indecipherable to unauthorized persons, was
13 viewed by unauthorized persons.

14 69. Plaintiffs' and Class Members' unsecured PHI was viewed by unauthorized persons
15 in a manner not permitted under 45 CFR, Subpart E as a result of the Data Breach.

16 70. Defendant reasonably believes that Plaintiffs' and Class Members' unsecured PHI
17 was viewed by unauthorized persons in a manner not permitted under 45 CFR, Subpart E as a
18 result of the Data Breach.

19 71. It is reasonable to infer that Plaintiffs' and Class Members' unsecured PHI that was
20 acquired, accessed, used, and/or disclosed in a manner not permitted under 45 CFR, Subpart E as
21 a result of the Data Breach, and which was not rendered unusable, unreadable, or indecipherable
22 to unauthorized persons, was viewed by unauthorized persons.

23 72. It should be rebuttably presumed that unsecured PHI acquired, accessed, used,
24 and/or disclosed in a manner not permitted under 45 CFR, Subpart E, and which was not rendered
25 unusable, unreadable, or indecipherable to unauthorized persons, was viewed by unauthorized
26 persons.

73. After receiving notice that they were victims of the Data Breach (which required the filing of a data breach report in accordance with 45 CFR § 164.408(a)), it is reasonable for recipients of that notice, including Plaintiffs and Class Members in this case, to believe that future harm (including medical identity theft) is real and imminent, and to take steps necessary to mitigate that risk of future harm.

74. Defendant's security failures also include, but are not limited to:

- a. Failing to maintain adequate data security systems, practices, and protocols to prevent data loss;
- b. Failing to mitigate the risks of a data breach and loss of data;
- c. Failing to ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity *or business associate* creates, receives, maintains, or transmits" and "protect against any reasonably anticipated threats or hazards to the security or integrity of such information," in violation of 45 C.F.R. § 164.306 (emphasis added).
- d. Failing to ensure the confidentiality and integrity of electronic protected health information Defendant creates, receives, maintains, and transmits in violation of 45 CFR 164.306(a)(1);
- e. Failing to implement policies and procedures to prevent, detect, contain, and correct security violations in violation of 45 CFR 164.308(a)(1);
- f. Failing to mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, in violation of 45 CFR 164.308(a)(6)(ii);
- g. Failing to protect against any reasonably-anticipated threats or hazards to the security or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2);
- h. Failing to protect against any reasonably anticipated uses or disclosures of electronic protected health information that are not permitted under the privacy

rules regarding individually identifiable health information, in violation of 45 CFR 164.306(a)(3); and

- i. Impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

75. Because Defendant failed to comply with HIPAA, while monetary relief may cure some of Plaintiffs' and Class Members' injuries, injunctive relief is also necessary to ensure Defendant's approach to information security, especially as such approach relates to the supervision of its business associates, vendors, and/or suppliers, is adequate and appropriate going forward. Defendant still maintains the PHI and other highly sensitive PII of its current and former patients. Without the supervision of the Court through injunctive relief, Plaintiffs' and Class Members' Private Information remains at risk of subsequent data breaches.

E. Defendant Failed to Comply with FTC Guidelines

76. The Federal Trade Commission ("FTC") has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making. Indeed, the FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45. *See, e.g., FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

77. In October 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established cybersecurity guidelines for businesses. The guidelines note that businesses should protect the personal customer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating

1 someone is attempting to hack into the system, watch for large amounts of data being transmitted
2 from the system, and have a response plan ready in the event of a breach.

3 78. The FTC further recommends that companies not maintain PII longer than is
4 needed for authorization of a transaction, limit access to sensitive data, require complex passwords
5 to be used on networks, use industry-tested methods for security, monitor the network for
6 suspicious activity, and verify that third-party service providers have implemented reasonable
7 security measures.

8 79. The FTC has brought enforcement actions against businesses for failing to
9 adequately and reasonably protect customer data by treating the failure to employ reasonable and
10 appropriate measures to protect against unauthorized access to confidential consumer data as an
11 unfair act or practice prohibited by the FTCA. Orders resulting from these actions further clarify
12 the measures businesses must take to meet their data security obligations.

13 80. As evidenced by the Data Breach, Defendant failed to properly implement basic
14 data security practices. Defendant's failure to employ reasonable and appropriate measures to
15 protect against unauthorized access to Plaintiffs' and Class Members' Private Information
16 constitutes an unfair act or practice prohibited by Section 5 of the FTCA.

17 81. Defendant was at all times fully aware of its obligations to protect the Private
18 Information of its patients yet failed to comply with such obligations. Defendant was also aware
19 of the significant repercussions that would result from its failure to do so.

20 **F. Defendant Breached Its Duty to Safeguard Plaintiffs' and Class Members' Private**
21 **Information**

22 82. In addition to its obligations under federal and state laws, Defendant owed a duty
23 to Plaintiffs and Class Members to exercise reasonable care in obtaining, retaining, securing,
24 safeguarding, deleting, and protecting the Private Information in its possession from being
25 compromised, lost, stolen, accessed, and misused by unauthorized persons. Defendant owed a duty
26 to Plaintiffs and Class Members to provide reasonable security, including consistency with
27 industry standards and requirements, and to ensure that its computer systems, networks, and
28

1 protocols (and those of its business associates, vendors, and/or suppliers) adequately protected the
2 Private Information of Class Members.

3 83. Defendant breached its obligations to Plaintiffs and Class Members and/or was
4 otherwise negligent and reckless because it failed to properly maintain and safeguard its computer
5 systems and data (and those of its business associates, vendors, and/or suppliers). Defendant's
6 unlawful conduct includes, but is not limited to, the following acts and/or omissions:

- 7 a. Failing to adequately protect Class Members' Private Information;
- 8 b. Failing to sufficiently train and monitor its business associates, vendors, and/or
9 suppliers regarding the proper handling of its patients' Private Information;
- 10 c. Failing to fully comply with FTC guidelines for cybersecurity in violation of the
11 FTCA;
- 12 d. Failing to adhere to HIPAA and industry standards for cybersecurity, as discussed
13 above; and
- 14 e. Otherwise breaching its duties and obligations to protect Plaintiffs' and Class
15 Members' Private Information.

16 84. Had Defendant remedied the deficiencies in its information storage and security
17 practices, procedures, and protocols, followed industry guidelines, and adopted security measures
18 recommended by experts in the field, they could have prevented the theft of Plaintiffs' and Class
19 Members' confidential Private Information.

20 85. Accordingly, Plaintiffs' and Class Members' lives were severely disrupted. What's
21 more, they have been harmed as a result of the Data Breach and now face an increased risk of
22 future harm that includes, but is not limited to, fraud and identity theft.

23 **G. Defendant Should Have Known that Cybercriminals Target PII and PHI to Carry**
24 **Out Fraud and Identity Theft**

25 86. The FTC hosted a workshop to discuss "informational injuries," which are injuries
26 that consumers like Plaintiffs and Class Members suffer from privacy and security incidents such
27
28

1 as data breaches or unauthorized disclosure of data.¹⁶ Exposure of highly sensitive personal
 2 information that a consumer wishes to keep private may cause harm to the consumer, such as the
 3 ability to obtain or keep employment. Consumers' loss of trust in e-commerce also deprives them
 4 of the benefits provided by the full range of goods and services available which can have negative
 5 impacts on daily life.

6 87. Any victim of a data breach is exposed to serious ramifications regardless of the
 7 nature of the data that was breached. Indeed, the reason why criminals steal information is to
 8 monetize it. They do this by selling the spoils of their cyberattacks on the black market to identity
 9 thieves who desire to extort and harass victims or to take over victims' identities in order to engage
 10 in illegal financial transactions under the victims' names.

11 88. Because a person's identity is akin to a puzzle, the more accurate pieces of data an
 12 identity thief obtains about a person, the easier it is for the thief to take on the victim's identity or
 13 to otherwise harass or track the victim. For example, armed with just a name and date of birth, a
 14 data thief can utilize a hacking technique referred to as "social engineering" to obtain even more
 15 information about a victim's identity, such as a person's login credentials or Social Security
 16 number. Social engineering is a form of hacking whereby a data thief uses previously acquired
 17 information to manipulate individuals into disclosing additional confidential or personal
 18 information through means such as spam phone calls and text messages or phishing emails.

19 89. In fact, as technology advances, computer programs may scan the Internet with a
 20 wider scope to create a mosaic of information that may be used to link compromised information
 21 to an individual in ways that were not previously possible. This is known as the "mosaic effect."
 22 Names and dates of birth, combined with contact information like telephone numbers and email
 23

24 ¹⁶ *FTC Information Injury Workshop, BE and BCP Staff Perspective*, Federal Trade
 25 Commission, (October 2018), available at
 26 [https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf)
 27 [staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf](https://www.ftc.gov/system/files/documents/reports/ftc-informational-injury-workshop-be-bcp-staff-perspective/informational_injury_workshop_staff_report_-_oct_2018_0.pdf) (last visited on
 28 Sept. 19, 2023).

1 addresses, are very valuable to hackers and identity thieves as it allows them to access users' other
2 accounts.

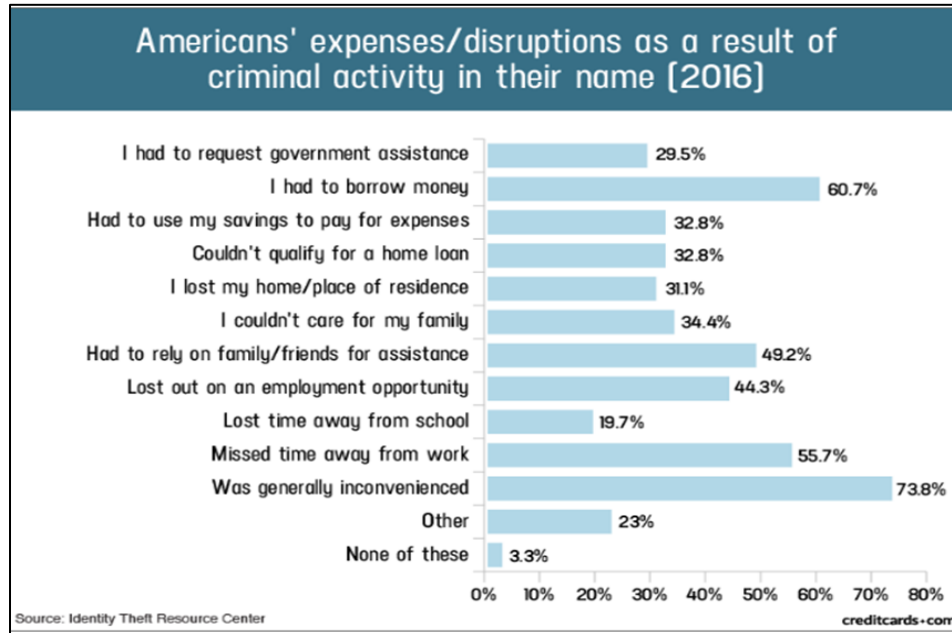
3 90. Thus, even if certain information was not purportedly involved in the Data Breach,
4 the unauthorized parties could use Plaintiffs' and Class Members' Private Information to access
5 accounts, including, but not limited to, email accounts and financial accounts, to engage in a wide
6 variety of fraudulent activity against Plaintiffs and Class Members.

7 91. For these reasons, the FTC recommends that identity theft victims take several
8 time-consuming steps to protect their personal and financial information after a data breach,
9 including contacting one of the credit bureaus to place a fraud alert on their account (and an
10 extended fraud alert that lasts for 7 years if someone steals the victim's identity), reviewing their
11 credit reports, contacting companies to remove fraudulent charges from their accounts, placing a
12 freeze on their credit, and correcting their credit reports.¹⁷ However, these steps do not guarantee
13 protection from identity theft but can only mitigate identity theft's long-lasting negative impacts.

14 92. Identity thieves can also use stolen personal information such as Social Security
15 numbers and PHI for a variety of crimes, including credit card fraud, phone or utilities fraud, bank
16 fraud, to obtain a driver's license or official identification card in the victim's name but with the
17 thief's picture, to obtain government benefits, or to file a fraudulent tax return using the victim's
18 information. In addition, identity thieves may obtain a job using the victim's Social Security
19 number, rent a house in the victim's name, receive medical services in the victim's name, and even
20 give the victim's personal information to police during an arrest resulting in an arrest warrant being
21 issued in the victim's name.

22
23
24
25
26
27 ¹⁷ See *IdentityTheft.gov*, Federal Trade Commission, available at
28 <https://www.identitytheft.gov/Steps> (last visited Sept. 19, 2023).

93. In fact, a study by the Identity Theft Resource Center¹⁸ shows the multitude of harms caused by fraudulent use of PII:



94. PHI is also especially valuable to identity thieves. As the FTC recognizes, identity thieves can use PHI to commit an array of crimes, including identity theft and medical and financial fraud.¹⁹

95. Indeed, a robust cyber black market exists in which criminals openly post stolen PHI on multiple underground Internet websites, commonly referred to as the dark web.

¹⁸ Steele, Jason, *Credit Card and ID Theft Statistics*, CreditCards.com (October 23, 2017), available at <https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276/> (last visited on Sept. 19, 2023).

¹⁹ Federal Trade Commission, *Warning Signs of Identity Theft*, available at: <https://consumer.ftc.gov/articles/what-know-about-identity-theft> (last visited on Sept. 19, 2023).

1 96. While credit card information and associated PII can sell for as little as \$1-\$2 on
2 the black market, protected health information can sell for as much as \$363 according to the
3 Infosec Institute.²⁰

4 97. PHI is particularly valuable because criminals can use it to target victims with
5 frauds and scams that take advantage of the victim's medical conditions or victim settlements. It
6 can be used to create fake insurance claims, allowing for the purchase and resale of medical
7 equipment, or gain access to prescriptions for illegal use or resale.

8 98. Medical identity theft can result in inaccuracies in medical records and costly false
9 claims. It can also have life-threatening consequences. If a victim's health information is mixed
10 with other records, it can lead to misdiagnosis or mistreatment. "Medical identity theft is a growing
11 and dangerous crime that leaves its victims with little to no recourse for recovery," reported Pam
12 Dixon, executive director of World Privacy Forum. "Victims often experience financial
13 repercussions and worse yet, they frequently discover erroneous information has been added to
14 their personal medical files due to the thief's activities."²¹

15 99. The ramifications of Defendant's failure to keep its patients' Private Information
16 secure are long lasting and severe. Once it is stolen, fraudulent use of such and damage to victims
17 may continue for years.

18 100. Here, not only was sensitive medical information compromised, but Social Security
19 numbers may have been compromised too. The value of both PII and PHI is axiomatic. The value
20 of "big data" in corporate America is astronomical. The fact that identity thieves attempt to steal
21
22

23 ²⁰ Center for Internet Security, *Data Breaches: In the Healthcare Sector*, available at:
24 <https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector> (last visited on
25 Sept. 19, 2023).

26 ²¹ Michael Ollove, "The Rise of Medical Identity Theft in Healthcare," Kaiser Health News, Feb.
27 7, 2014, available at: <https://kffhealthnews.org/news/rise-of-indentity-theft/> (last visited on Sept.
28 19, 2023).

identities notwithstanding possible heavy prison sentences illustrates beyond a doubt that the Private Information compromised here has considerable market value.

101. It must also be noted that there may be a substantial time lag between when harm occurs and when it is discovered, and between when PII and/or PHI is stolen and when it is misused. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:²²

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.

102. PII and PHI are such valuable commodities to identity thieves that once the information has been compromised, criminals often trade the information on the dark web for years.

103. As a result, Plaintiffs and Class Members are at an increased risk of fraud and identity theft, including medical identity theft, for many years into the future. Thus, Plaintiffs and Class Members have no choice but to vigilantly monitor their accounts for many years to come.

H. Plaintiffs' and Class Members' Damages

Plaintiff Rosa's Experience

104. Plaintiff Rosa first learned of the Breach when he received a notice email (substantially similar to the Notice) from his employer.

105. Upon information and belief, Brightline obtained Plaintiff Rosa's PII and PHI from his employer, which used Brightline to deliver health services.

²² *Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (June 2007), available at <https://www.gao.gov/assets/270/262904.html> (last visited Sept. 19, 2023).

1 106. Soon after and as a result of the Data Breach, Plaintiff Rosa experienced an increase
2 in spam and suspicious phone calls, texts, and emails. He was also alerted through his credit
3 monitoring service that his Private Information is now on the dark web.

4 107. As a result of the Data Breach and at the recommendation of Brightline and its
5 Notice, Plaintiff Rosa made reasonable efforts to mitigate the impact of the Data Breach, including
6 but not limited to, researching the Data Breach, reviewing credit card and financial account
7 statements, changing his online account passwords, and monitoring his credit information.

8 108. Plaintiff Rosa has spent significant time responding to the Data Breach and will
9 continue to spend valuable time he otherwise would have spent on other activities, including but
10 not limited to work and/or recreation.

11 109. Plaintiff Rosa suffered lost time, annoyance, interference, and inconvenience as a
12 result of the Data Breach and has experienced anxiety and increased concerns for the loss of his
13 privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI
14 and/or financial information.

15 110. Plaintiff Rosa is now subject to the present and continuing risk of fraud, identity
16 theft, and misuse resulting from their PII and PHI, in combination with his name, being placed in
17 the hands of unauthorized third parties/criminals.

18 111. Plaintiff Rosa has a continuing interest in ensuring that his PII and PHI which, upon
19 information and belief, remains in Brightline's possession, is protected and safeguarded from
20 future breaches.

21 *Plaintiff Watson's Experience*

22 112. Plaintiff Watson first found out about the Breach when he reviewed a notice email
23 (substantially similar to the Notice) that he received from his employer.

24 113. Upon information and belief, Brightline obtained Plaintiff Watson's PII and PHI
25 from his employer, which used the company to deliver health services.

26 114. Shortly after and as a result of the Data Breach, Plaintiff Watson received a
27 fraudulent call where the caller attempted to elicit banking information from him. This caller
28

1 pretended to be an Amazon representative who needed to verify his banking information for a
2 pending delivery. In actuality, there was no pending delivery as Plaintiff Watson had made no such
3 purchase. This was just one of the many spam and suspicious phone calls, texts, and emails
4 Plaintiff Watson received as a result of the Data Breach.

5 115. Plaintiff Watson made reasonable efforts to mitigate the impact of the Data Breach,
6 including but not limited to, researching the Data Breach, reviewing credit card and financial
7 account statements, changing his online account passwords, and monitoring his credit information.

8 116. Plaintiff Watson has spent significant time responding to the Data Breach and will
9 continue to spend valuable time dealing with the effects of the Data Breach, time that he otherwise
10 would have spent on other activities.

11 117. Plaintiff Watson suffered lost time, annoyance, interference, and inconvenience as
12 a result of the Data Breach and has experienced anxiety and increased concerns for the loss of his
13 privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI
14 for fraudulent purposes.

15 118. Plaintiff Watson is now subject to the present and continuing risk of fraud, identity
16 theft, and misuse resulting from his PII and PHI, in combination with his name, being placed in
17 the hands of unauthorized third parties/criminals.

18 119. Plaintiff Watson has a continuing interest in ensuring that his PII and PHI which,
19 upon information and belief, remains in Brightline's possession, is protected and safeguarded from
20 future breaches.

21 *Plaintiff Ndifor's Experience*

22 120. Plaintiff Ndifor first learned about the Breach from a notice email (substantially
23 similar to the Notice) sent by his employer.

24 121. Upon information and belief, Brightline obtained Plaintiff Ndifor's PII and PHI
25 from his employer, which used the website to deliver health services.

1 122. Like the other Plaintiffs, following the Data Breach, Plaintiff Ndifor experienced
2 an increase in spam and suspicious phone calls, texts, and emails. Like Plaintiff Rosa, Plaintiff
3 Ndifor's credit monitoring service alerted him that his Private Information is now on the dark web.

4 123. As a result of the Data Breach, Plaintiff Ndifor made reasonable efforts to mitigate
5 the impact of the Data Breach, including but not limited to, researching the Data Breach, reviewing
6 credit card and financial account statements, changing his online account passwords, and
7 monitoring his credit information.

8 124. Plaintiff Ndifor has spent significant time responding to the Data Breach and will
9 continue to spend valuable time he otherwise would have spent on other activities, including but
10 not limited to work and/or recreation.

11 125. Plaintiff Ndifor suffered lost time, annoyance, interference, and inconvenience as a
12 result of the Data Breach and has experienced anxiety and increased concerns for the loss of his
13 privacy, as well as anxiety over the impact of cybercriminals accessing and using his PII and PHI
14 and/or financial information.

15 126. Plaintiff Ndifor is now subject to the present and continuing risk of fraud, identity
16 theft, and misuse resulting from their PII and PHI, in combination with his name, being placed in
17 the hands of unauthorized third parties/criminals.

18 127. Plaintiff Ndifor has a continuing interest in ensuring that his PII and PHI which,
19 upon information and belief, remains backed up in Brightline's possession, is protected and
20 safeguarded from future breaches.

21 *Plaintiff Jackson's Experience*

22 128. Plaintiff Jackson received the data breach notice letter from Brightline on or about
23 May 5, 2023.

24 129. Plaintiff Jackson has been damaged by the compromise of her Private Information
25 in the Data Breach.

26 130. Plaintiff Jackson entrusted her Private Information to Defendant in order to receive
27 Defendant's services.
28

1 131. Plaintiff Jackson's Private Information was subsequently compromised as a direct
2 and proximate result of the Data Breach, which Data Breach resulted from Defendant's inadequate
3 data security practices, procedures, and protocols, as discussed herein.

4 132. As a direct and proximate result of Defendant's actions and omissions, Plaintiff
5 Jackson has been harmed and is at an imminent, immediate, and continuing increased risk of harm,
6 including but not limited to, having medical services billed in her name, loans opened in her name,
7 tax returns filed in her name, utility bills opened in her name, credit card accounts opened in her
8 name, and other forms of identity theft.

9 133. Further, as a direct and proximate result of the Data Breach, Plaintiff Jackson has
10 been forced to spend time dealing with and attempting to mitigate the negative effects thereof.

11 134. Plaintiff Jackson also faces a substantial risk of being targeted in future phishing,
12 data intrusion, and other illegal schemes through the misuse of her Private Information, since
13 potential fraudsters will likely use such Private Information to carry out such targeted schemes
14 against Plaintiff Jackson as they already have other Class Members.

15 135. The Private Information maintained by and stolen from Defendant's system,
16 combined with publicly available information, allows nefarious actors to assemble a detailed
17 mosaic of Plaintiff Jackson, which can also be used to carry out targeted medical fraud and/or
18 identity theft against her.

19 136. Additionally, Plaintiff Jackson has spent and will continue to spend significant
20 amounts of time monitoring her accounts and records, including medical records and explanations
21 of benefits, for misuse.

22 137. Plaintiff Jackson has suffered or will suffer actual injury as a direct and proximate
23 result of the Data Breach in the form of out-of-pocket expenses and the value of her time
24 reasonably incurred to remedy or mitigate the effects of the Data Breach.

25 138. Moreover, Plaintiff Jackson has an interest in ensuring that her Private Information,
26 which is believed to still be in the possession of Defendant, is protected from future breaches by
27 the implementation of appropriate data security measures and safeguards.
28

1 139. As a direct and proximate result of Defendant's actions and inactions, Plaintiff
2 Jackson has suffered a loss of privacy and cognizable harm, including an imminent and substantial
3 future risk of harm, in the forms set forth above.

4 *Plaintiff Castro's Experience*

5 140. Plaintiff Castro received the data breach notice letter from Brightline on or about
6 May 5, 2023.

7 141. Plaintiff Castro has been damaged by the compromise of his Private Information in
8 the Data Breach.

9 142. Plaintiff Castro entrusted his Private Information, along with that of his minor
10 children, to Defendant in order to receive Defendant's services.

11 143. Plaintiff Castro's and his children's Private Information was subsequently
12 compromised as a direct and proximate result of the Data Breach, which Data Breach resulted from
13 Defendant's inadequate data security practices, procedures, and protocols, as discussed herein.

14 144. As a direct and proximate result of Defendant's actions and omissions, Plaintiff
15 Castro and his children have been harmed and are at an imminent, immediate, and continuing
16 increased risk of harm, including but not limited to, having medical services billed in their names,
17 loans opened in their names, tax returns filed in their names, utility bills opened in their names,
18 credit card accounts opened in their names, and other forms of identity theft.

19 145. Further, as a direct and proximate result of the Data Breach, Plaintiff Castro has
20 been forced to spend time dealing with and attempting to mitigate the negative effects thereof. For
21 example, in an effort to mitigate the heightened risk of identity theft and fraud that he and his
22 children now face, Plaintiff Castro has subscribed to a paid online credit monitoring service
23 through IDshield. While this credit monitoring service allows Plaintiff Castro to monitor his and
24 his children's credit reports to determine whether suspicious activity has occurred, it is powerless
25 to stop identity theft in advance and does not indemnify them from, or insure them against, the
26 harm caused by the Data Breach.

1 146. Plaintiff Castro has also expended considerable time and effort attempting to
2 contact Brightline and monitoring his and his children's identity and credit reports periodically, in
3 addition to gathering documentation relating to the same.

4 147. Plaintiff Castro further faces a substantial risk of being targeted in future phishing,
5 data intrusion, and other illegal schemes through the misuse of his Private Information, since
6 potential fraudsters will likely use such Private Information to carry out such targeted schemes
7 against Plaintiff Castro as they already have other Class Members.

8 148. The Private Information maintained by and stolen from Defendant's system,
9 combined with publicly available information, allows nefarious actors to assemble a detailed
10 mosaic of Plaintiff Castro, which can also be used to carry out targeted medical fraud and/or
11 identity theft against him.

12 149. Additionally, Plaintiff Castro has spent and will continue to spend significant
13 amounts of time monitoring his accounts and records, including medical records and explanations
14 of benefits, for misuse.

15 150. Plaintiff Castro has suffered or will suffer actual injury as a direct and proximate
16 result of the Data Breach in the form of out-of-pocket expenses and the value of his time reasonably
17 incurred to remedy or mitigate the effects of the Data Breach.

18 151. Moreover, Plaintiff Castro has an interest in ensuring that his Private Information
19 and that of his children, which is believed to still be in the possession of Defendant, is protected
20 from future breaches by the implementation of appropriate data security measures and safeguards.

21 152. As a direct and proximate result of Defendant's actions and inactions, Plaintiff
22 Castro has suffered a loss of privacy and cognizable harm, including an imminent and substantial
23 future risk of harm, in the forms set forth above.

24 *Plaintiff Milner's Experience*

25 153. Plaintiff Milner received the data breach notice letter from Brightline on or about
26 May 5, 2023.

1 154. Plaintiff Milner has been damaged by the compromise of her Private Information
2 in the Data Breach.

3 155. Plaintiff Milner entrusted her Private Information, along with that of her minor
4 child, to Defendant in order to receive Defendant's services.

5 156. Plaintiff Milner's and her minor child's Private Information was subsequently
6 compromised as a direct and proximate result of the Data Breach, which resulted from Defendant's
7 inadequate data security practices, procedures, and protocols, as discussed herein.

8 157. As a direct and proximate result of Defendant's actions and omissions, Plaintiff
9 Milner and her child have been harmed and are at an imminent, immediate, and continuing
10 increased risk of harm, including but not limited to, having medical services billed in their names,
11 loans opened in their names, tax returns filed in their names, utility bills opened in their names,
12 credit card accounts opened in their names, and other forms of identity theft.

13 158. Further, as a direct and proximate result of the Data Breach, Plaintiff Milner has
14 been forced to spend time dealing with and attempting to mitigate the negative effects thereof.

15 159. Plaintiff Milner also faces a substantial risk of being targeted in future phishing,
16 data intrusion, and other illegal schemes through the misuse of her Private Information, since
17 potential fraudsters will likely use such Private Information to carry out such targeted schemes
18 against Plaintiff Milner as they already have other Class Members.

19 160. The Private Information maintained by and stolen from Defendant's system,
20 combined with publicly available information, allows nefarious actors to assemble a detailed
21 mosaic of Plaintiff Milner, which can also be used to carry out targeted medical fraud and/or
22 identity theft against her.

23 161. Additionally, Plaintiff Milner has spent and will continue to spend significant
24 amounts of time monitoring her accounts and records, including medical records and explanations
25 of benefits, for misuse.

162. Plaintiff Milner has suffered or will suffer actual injury as a direct and proximate result of the Data Breach in the form of out-of-pocket expenses and the value of her time reasonably incurred to remedy or mitigate the effects of the Data Breach.

163. Moreover, Plaintiff Milner has an interest in ensuring that her Private Information and that of her child, which is believed to still be in the possession of Defendant, is protected from future breaches by the implementation of appropriate data security measures and safeguards.

164. As a direct and proximate result of Defendant's actions and inactions, Plaintiff Milner has suffered a loss of privacy and cognizable harm, including an imminent and substantial future risk of harm, in the forms set forth above.

V. CLASS ACTION ALLEGATIONS

165. Plaintiffs bring this action individually and on behalf of all other persons similarly situated, pursuant to Fed. R. Civ. P. 23.

166. Specifically, Plaintiffs propose the following Nationwide Class and state subclasses, subject to amendment as appropriate:

Nationwide Class

All persons, including minor children, residing in the United States who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

California Subclass

All persons, including minor children, residing in California who had Private Information accessed and/or acquired as a result of the Data Breach, including all who were sent a notice of the Data Breach.

Illinois Subclass

1 All persons, including minor children, residing in Illinois who had
 2 Private Information accessed and/or acquired as a result of the Data
 3 Breach, including all who were sent a notice of the Data Breach.

4 **Tennessee Subclass**

5 All persons, including minor children, residing in Tennessee who
 6 had Private Information accessed and/or acquired as a result of the
 7 Data Breach, including all who were sent a notice of the Data
 8 Breach.

9 **Virginia Subclass**

10 All persons, including minor children, residing in Virginia who had
 11 Private Information accessed and/or acquired as a result of the Data
 12 Breach, including all who were sent a notice of the Data Breach.

13 **Pennsylvania Subclass**

14 All persons, including minor children, residing in Pennsylvania who
 15 had Private Information accessed and/or acquired as a result of the
 16 Data Breach, including all who were sent a notice of the Data
 17 Breach.

18 **New Jersey Subclass**

19 All persons, including minor children, residing in New Jersey who
 20 had Private Information accessed and/or acquired as a result of the
 21 Data Breach, including all who were sent a notice of the Data
 22 Breach.

23 (the California Subclass, Illinois Subclass, Tennessee Subclass, Virginia Subclass, Pennsylvania
 24 Subclass, and New Jersey Subclass are collectively the “State Subclasses”, and collectively the
 25 Nationwide Class and State Subclasses are referred to herein as the “Class”).

26 167. Excluded from the Class are Defendant and its parents or subsidiaries, any entities
 27 in which they have a controlling interest, as well as its officers, directors, affiliates, legal
 28

representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

168. Plaintiffs reserve the right to modify or amend the definition of the proposed Class or add additional subclasses before the Court determines whether certification is appropriate.

169. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Though the exact identities of Class Members are unknown at this time, based on information and belief, the Class consists of nearly 1 million individuals whose data was compromised in the Data Breach. The identities of Class Members are ascertainable through Defendant's records, Class Members' records, publication notice, self-identification, and other means.

170. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These common questions of law and fact include, without limitation:

- a. Whether Defendant engaged in the conduct alleged herein;
- b. Whether Defendant's conduct violated the FTCA, HIPAA, and/or state consumer protection laws and/or privacy laws;
- c. Whether and to what extent Defendant had a duty to protect the Private Information of Class Members;
- d. When Defendant learned of the vulnerability within its network that led to the Data Breach;
- e. Whether Defendant's response to the Data Breach was adequate;
- f. Whether Defendant took reasonable steps and measures to safeguard Plaintiffs' and Class Members' Private Information;
- g. Whether Defendant breached its duty to Class Members to safeguard their Private Information;
- h. Whether hackers obtained Class Members' Private Information via the Data Breach;

- i. Whether Defendant knew or should have known that its data monitoring and supervision processes were deficient;
- j. Whether Defendant was aware that its business associates', vendors', and/or suppliers' data security practices, procedures, and protocols were inadequate;
- k. What damages Plaintiffs and Class Members suffered as a result of Defendant's misconduct;
- l. Whether Defendant's conduct was negligent;
- m. Whether Defendant was unjustly enriched;
- n. Whether Plaintiffs and Class Members are entitled to actual and/or statutory damages;
- o. Whether Plaintiffs and Class Members are entitled to lifetime credit or identity monitoring and monetary relief; and
- p. Whether Plaintiffs and Class Members are entitled to equitable relief, including injunctive relief, restitution, disgorgement, and/or the establishment of a constructive trust.

171. Typicality. Plaintiffs' claims are typical of those of other Class Members because Plaintiffs' Private Information, like that of every other Class Member, was compromised in the Data Breach. Plaintiffs' claims are typical of those of the other Class Members because, *inter alia*, all Class Members were injured through the common misconduct of Defendant. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of Class Members arise from the same operative facts and are based on the same legal theories.

172. Adequacy of Representation. Plaintiffs will fairly and adequately represent and protect the interests of Class Members. Plaintiffs' counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

1 173. Predominance. Defendant has engaged in a common course of conduct toward
2 Plaintiffs and Class Members in that all of Plaintiffs' and Class Members' data was stored on the
3 same computer systems and unlawfully accessed and exfiltrated in the same way and as a result of
4 the same negligent acts and omissions committed by Defendant. The common issues arising from
5 Defendant's conduct affecting Class Members set out above predominate over any individualized
6 issues. Adjudication of these common issues in a single action has important and desirable
7 advantages of judicial economy.

8 174. Superiority. A Class action is superior to other available methods for the fair and
9 efficient adjudication of this controversy and no unusual difficulties are likely to be encountered
10 in the management of this class action. Class treatment of common questions of law and fact is
11 superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class
12 Members would likely find that the cost of litigating their individual claims is prohibitively high
13 and would therefore have no effective remedy. The prosecution of separate actions by individual
14 Class Members would create a risk of inconsistent or varying adjudications with respect to
15 individual Class Members, which would establish incompatible standards of conduct for
16 Defendant. In contrast, conducting this action as a class action presents far fewer management
17 difficulties, conserves judicial resources and the parties' resources, and protects the rights of each
18 Class Member.

19 175. Defendant has acted and/or refused to act on grounds generally applicable to the
20 Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to
21 the Class as a whole.

22 176. Finally, all members of the proposed Class are readily ascertainable. Defendant has
23 access to the names and addresses and/or email addresses of Class Members affected by the Data
24 Breach. Class Members have already been preliminarily identified and sent notice of the Data
25 Breach by Defendant.
26
27
28

VI. CLAIMS FOR RELIEF

COUNT I

NEGLIGENCE AND/OR NEGLIGENCE PER SE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

177. Plaintiffs restate and reallege all of the allegations in the preceding paragraphs as if fully set forth herein.

178. Defendant knowingly collected, came into possession of, and maintained Plaintiffs' and Class Members' Private Information, and had a duty to exercise reasonable care in safeguarding, securing, and protecting such Information from being disclosed, compromised, lost, stolen, and misused by unauthorized parties.

179. Defendant knew or should have known of the risks inherent in collecting the Private Information of Plaintiffs and Class Members and the importance of adequate security. Defendant was on notice because, on information and belief, it knew or should have known that the Private Information would be an attractive target for cyberattacks.

180. Defendant owed a duty of care to Plaintiffs and Class Members whose Private Information was entrusted to them. Defendant's duties included, but were not limited to, the following:

- a. To exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, supervising, monitoring, and protecting the Private Information in its possession;
- b. To protect patients' and client's employees' Private Information using reasonable and adequate security procedures and systems compliant with industry standards;
- c. To have procedures, including but not limited to monitoring and supervision procedures, in place to prevent the loss or unauthorized dissemination of Private Information in its possession;

d. To employ reasonable security measures and otherwise protect the Private Information of Plaintiffs and Class Members pursuant to HIPAA, the FTCA, and California's Unfair Competition Law;

e. To implement processes to quickly detect a data breach and to timely act on warnings about data breaches; and

f. To promptly notify Plaintiffs and Class Members of the Data Breach, and to precisely disclose the type(s) of information compromised.

181. Defendant's duty to employ reasonable data security measures arose, in part, under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

182. Moreover, under HIPAA, Brightline had a duty to use reasonable security measures to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information."²³ Some or all of the medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.²⁴

183. Brightline also had a duty under HIPAA to render the electronic PII and PHI that it maintained as unusable, unreadable, or indecipherable to unauthorized individuals. Specifically, the HIPAA Security Rule requires "the use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key."²⁵

184. Plaintiffs and Class Members are within the class of persons that the FTCA and HIPAA were intended to protect. And the injuries that Brightline inflicted on Plaintiffs and Class Members are precisely the harms that the FTCA and HIPAA guards against. After all, the Federal

²³ 45 C.F.R. § 164.530(c)(1).

²⁴ *Id.*

²⁵ 45 C.F.R. § 164.304 (defining encryption).

1 Trade Commission and the Federal Health and Human Services' Office for Civil Rights ("OCR")
2 have pursued enforcement actions against businesses which—because of their failure to employ
3 reasonable data security measures for PII and/or PHI— caused the very same injuries that
4 Brightline inflicted upon Plaintiffs and Class Members.

5 185. Under § 17932 of the Health Information Technology for Economic and Clinical
6 Health Act ("HITECH"), Brightline have duty to promptly notify "without unreasonable delay and
7 in no case later than 60 calendar days after the discovery of a breach" the respective covered
8 entities and affected persons so that the entities and persons can take action to protect themselves.²⁶

9 186. Additionally, § 17932(a) of HITECH states that, "[a] covered entity that accesses,
10 maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses
11 unsecured protected health information (as defined in subsection (h)(1)) shall, in the case of a
12 breach of such information that is discovered by the covered entity, notify each individual whose
13 unsecured protected health information has been, or is reasonably believed by the covered entity
14 to have been, accessed, acquired, or disclosed as a result of such breach."

15 187. And § 17932(b) of HITECH states that, "[a] business associate of a covered entity
16 that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or
17 discloses unsecured protected health information shall, following the discovery of a breach of such
18 information, notify the covered entity of such breach. Such notice shall include the identification
19 of each individual whose unsecured protected health information has been or is reasonably
20 believed by the business associate to have been, accessed, acquired, or disclosed during such
21 breach."

22 188. Brightline's duty to use reasonable care in protecting confidential data arose not
23 only because of the statutes and regulations described above, but also because Brightline are bound
24 by industry standards to protect confidential PII and PHI.

25
26
27 ²⁶ 42 U.S.C.A. § 17932(d)(1).
28

1 189. Brightline owed Plaintiffs and Class Members a duty to notify them within a
2 reasonable time frame of any breach to their PII and PHI. Brightline also owed a duty to timely
3 and accurately disclose to Plaintiffs and Class Members the scope, nature, and occurrence of the
4 Data Breach. This duty is necessary for Plaintiffs and Class Members to take appropriate measures
5 to protect their PII and PHI, to be vigilant in the face of an increased risk of harm, and to take other
6 necessary steps in an effort to mitigate the fallout of Brightline's Data Breach.

7 190. Brightline owed these duties to Plaintiffs and Class Members because they are
8 members of a well-defined, foreseeable, and probable class of individuals whom Brightline knew
9 or should have known would suffer injury-in-fact from its inadequate security protocols. After all,
10 Brightline actively sought and obtained the PII and PHI of Plaintiffs and Class Members.

11 191. Brightline breached their duties, and thus were negligent, by failing to use
12 reasonable measures to protect Plaintiffs' and Class Members' PII and PHI. And but for
13 Brightline's negligence, Plaintiffs and Class Members would not have been injured.

14 192. Defendant's duty also arose because Defendant was bound by industry standards to
15 protect its patients' and client's employees' confidential Private Information.

16 193. Plaintiffs and Class Members were foreseeable victims of any inadequate security
17 practices on the part of Defendant and its associates, vendors, and/or suppliers, and Defendant
18 owed Plaintiffs and Class Members a duty of care to not subject them to an unreasonable risk of
19 harm.

20 194. Defendant, through its actions and/or omissions, unlawfully breached its duty to
21 Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding
22 Plaintiffs' and Class Members' Private Information within its care.

23 195. Defendant, by its actions and/or omissions, breached its duty of care by failing to
24 provide, or acting with reckless disregard for, fair, reasonable, or adequate data security practices
25 to safeguard the Private Information of Plaintiffs and Class Members.

1 196. Defendant breached its duties, and thus was negligent, by failing to use reasonable
2 measures to protect Class Members' Private Information. The specific negligent acts and
3 omissions committed by Defendant include, but are not limited to, the following:

- 4 a. Failing to adopt, implement, and maintain adequate security measures to safeguard
5 Class Members' Private Information;
6 b. Failing to adequately monitor the security of the Private Information;
7 c. Allowing unauthorized access to Class Members' Private Information;
8 d. Failing to comply with the FTCA;
9 e. Failing to comply with HIPAA; and
10 f. Failing to comply with other state laws and regulations, as further set forth herein.

11 197. Defendant had a special relationship with Plaintiffs and Class Members. Plaintiffs'
12 and Class Members' willingness to entrust Defendant with their Private Information was
13 predicated on the understanding that Defendant would take adequate security precautions.

14 198. Defendant's breach of duties owed to Plaintiffs and Class Members caused
15 Plaintiffs' and Class Members' Private Information to be compromised, exfiltrated, and misused,
16 as alleged herein.

17 199. As a result of Defendant's ongoing failure to notify Plaintiffs and Class Members
18 regarding exactly what Private Information has been compromised, Plaintiffs and Class Members
19 have been unable to take the necessary precautions to prevent future fraud and mitigate damages.

20 200. Defendant's breaches of duty also caused a substantial, imminent risk to Plaintiffs
21 and Class Members of identity theft, loss of control over their Private Information, and/or loss of
22 time and money to monitor their accounts for fraud.

23 201. As a result of Defendant's negligence in breach of its duties owed to Plaintiffs and
24 Class Members, Plaintiffs and Class Members are in danger of imminent harm in that their Private
25 Information, which is still in the possession of third parties, will be used for fraudulent purposes.

1 210. As consideration, Plaintiffs and Class Members turned over valuable Private
2 Information to Defendant. Accordingly, Plaintiffs and Class Members bargained with Defendant
3 to securely maintain and store their Private Information.

4 211. Defendant accepted possession of Plaintiffs' and Class Members' Private
5 Information for the purpose of providing services to Plaintiffs and Class Members.

6 212. In delivering their Private Information to Defendant in exchange for Defendant's
7 offering of telehealth services, Plaintiffs and Class Members intended and understood that
8 Defendant would adequately safeguard the Private Information as part of those services.

9 213. Defendant's implied promises to Plaintiffs and Class Members include, but are not
10 limited to, (1) taking steps to ensure that anyone who is granted access to Private Information,
11 including its business associates, vendors, and/or suppliers, also protect the confidentiality of that
12 data; (2) taking steps to ensure that the Private Information that is placed in the control of its
13 business associates, vendors, and/or suppliers is restricted and limited to achieve an authorized
14 business purpose; (3) restricting access to qualified and trained employees, business associates,
15 vendors, and/or suppliers; (4) designing and implementing appropriate retention policies to protect
16 the Private Information against criminal data breaches; (5) applying or requiring proper
17 encryption; (6) implementing multifactor authentication for access; (7) complying with HIPAA
18 standards to make sure that Plaintiffs' and Class Members' PHI would remain protected; and (8)
19 taking other steps to protect against foreseeable data breaches.

20 214. Plaintiffs and Class Members would not have entrusted their Private Information to
21 Defendant in the absence of such an implied contract.

22 215. Had Defendant disclosed to Plaintiffs and the Class that it did not have adequate
23 data security and data supervisory practices to ensure the security of their sensitive data, Plaintiffs
24 and Class Members would not have provided their Private Information to Defendant.

25 216. As a provider of telehealth services, Defendant recognized (or should have
26 recognized) that Plaintiffs' and Class Member's Private Information is highly sensitive and must
27
28

1 be protected, and that this protection was of material importance as part of the bargain with
2 Plaintiffs and the Class.

3 217. Defendant violated these implied contracts by failing to employ reasonable and
4 adequate security measures to secure Plaintiffs' and Class Members' Private Information.
5 Defendant further breached these implied contracts by failing to comply with its promise to abide
6 by HIPAA.

7 218. Additionally, Defendant breached the implied contracts with Plaintiffs and Class
8 Members by failing to ensure the confidentiality and integrity of electronic protected health
9 information they created, received, maintained, and transmitted, in violation of 45 CFR
10 164.306(a)(1).

11 219. Defendant further breached the implied contracts with Plaintiffs and Class
12 Members by failing to implement policies and procedures to prevent, detect, contain, and correct
13 security violations, in violation of 45 CFR 164.308(a)(1).

14 220. Defendant further breached the implied contracts with Plaintiffs and Class
15 Members by failing to identify and respond to suspected or known security incidents; mitigate, to
16 the extent practicable, harmful effects of security incidents that are known to the covered entity,
17 in violation of 45 CFR 164.308(a)(6)(ii).

18 221. Defendant further breached the implied contracts with Plaintiffs and Class
19 Members by failing to protect against any reasonably anticipated threats or hazards to the security
20 or integrity of electronic protected health information, in violation of 45 CFR 164.306(a)(2).

21 222. Defendant further breached the implied contracts with Plaintiffs and Class
22 Members by failing to protect against any reasonably anticipated uses or disclosures of electronic
23 protected health information that are not permitted under the privacy rules regarding individually
24 identifiable health information, in violation of 45 CFR 164.306(a)(3).

25 223. Defendant further breached the implied contracts with Plaintiffs and Class
26 Members by failing to ensure compliance with the HIPAA security standard rules by its workforce
27 violations, in violation of 45 CFR 164.306(a)(94).

224. Defendant further breached the implied contracts with Plaintiffs and Class Members by impermissibly and improperly using and disclosing protected health information that is and remains accessible to unauthorized persons, in violation of 45 CFR 164.502, *et seq.*

225. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to design, implement, and enforce policies and procedures establishing physical administrative safeguards to reasonably safeguard protected health information, in violation of 45 CFR 164.530(c).

226. Defendant further breached the implied contracts with Plaintiffs and Class Members by failing to ensure the confidentiality, integrity, and availability of all electronic protected health information its business associate(s) “create, receive, maintain, or transmit” and “protect against any reasonably anticipated threats or hazards to the security or integrity of such information,” in violation of 45 C.F.R. § 164.306 (emphasis added).

227. Defendant further breached the implied contracts with Plaintiffs and Class Members by otherwise failing to safeguard Plaintiffs’ and Class Members’ PHI.

228. A meeting of the minds occurred, as Plaintiffs and Class Members agreed, *inter alia*, to provide accurate and complete Private Information and to pay Defendant in exchange for Defendant’s agreement to, *inter alia*, protect their Private Information.

229. Plaintiffs and Class Members have been damaged by Defendant’s conduct, including the harms and injuries arising from the Data Breach now and in the future, as alleged herein.

COUNT III

BREACH OF CONTRACT

(ON BEHALF OF PLAINTIFFS JACKSON, CASTRO, MILNER, AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

230. Plaintiffs restate and reallege all the allegations in paragraphs 1 through 176 as if fully set forth herein.

1 231. Brightline offered to provide pediatric behavioral health services to Plaintiffs and
2 Class Members (and their children) in exchange for payment and/or entrustment of their valuable
3 Private Information.

4 232. Plaintiffs and the Class accepted Brightline's offer to provide pediatric behavioral
5 health services by paying for them and/or entrusting Brightline with their valuable Private
6 Information in order to receive said treatment.

7 233. Brightline required Plaintiffs and Class Members (and their children) to provide
8 their Private Information, including names, addresses, Social Security numbers, health insurance
9 information and limited medical information, in order to receive services from Brightline.

10 234. Plaintiffs and Class Members exchanged valuable consideration – including money
11 and their valuable Private Information – with Brightline for services, a crucial part of which was
12 Brightline's promise to protect their Private Information from unauthorized disclosure.

13 235. In its Privacy Policy, Brightline expressly promised Plaintiffs and the Class that it
14 would only disclose their Private Information under certain circumstances, none of which relate to
15 the Data Breach.

16 236. Necessarily implicit in the agreement between Brightline and its patients, including
17 Plaintiffs and Class Members, was Brightline's obligation to use such Private Information for
18 business and treatment purposes only, to take reasonable steps to secure and safeguard that Private
19 Information, and not make disclosures of such Information to unauthorized third parties.

20 237. Further implicit in the agreement, Brightline was obligated to provide Plaintiffs,
21 their children, and the Class with prompt and adequate notice of any and all unauthorized access
22 and/or theft of their PII and/or PHI.

23 238. Neither Plaintiffs nor Class Members would have entrusted their (or their
24 children's) Private Information to Brightline in the absence of such an agreement with Brightline.

25 239. Brightline materially breached the implied contract(s) it entered into with Plaintiffs
26 and Class Members by failing to safeguard their Private Information and failing to notify them
27
28

1 promptly of the intrusion into its computer systems that compromised such Information. Brightline
2 further breached the implied contracts with Plaintiffs and Class Members by:

- 3 a. Failing to properly safeguard and protect Plaintiffs', their children's, and
4 Class Members' Private Information;
- 5 b. Failing to comply with industry standards as well as legal obligations that
6 are necessarily incorporated into the parties' agreement;
- 7 c. Failing to ensure the confidentiality and integrity of electronic Private
8 Information, including PHI, that Brightline created, received, maintained and
9 transmitted in violation of 45 C.F.R. § 164.306(a)(1).

10 240. The damages sustained by Plaintiffs and Class Members as described above were
11 the direct and proximate result of Brightline's material breaches of its agreements.

12 241. Plaintiffs, their children, and Class Members have performed as required under the
13 relevant agreements, or such performance was waived by the conduct of Brightline.

14 242. Under the laws of California, good faith is an element of every contract. All such
15 contracts impose upon each party a duty of good faith and fair dealing. The parties must act with
16 honesty in fact in the conduct or transactions concerned. Good faith and fair dealing, in connection
17 with executing contracts and discharging performance and other duties according to their terms,
18 means preserving the spirit—not merely the letter—of the bargain. Put differently, the parties to a
19 contract are mutually obligated to comply with the substance of their contract in addition to its
20 form.

21 243. Subterfuge and evasion violate the obligation of good faith in performance even
22 when an actor believes their conduct to be justified. Bad faith may be overt or may consist of
23 inaction, and fair dealing may require more than honesty.

24 244. Brightline failed to promptly advise Plaintiffs, their children, and the Class of the
25 Data Breach.

26 245. In these and other ways, Brightline violated its duty of good faith and fair dealing.
27
28

246. Plaintiffs, their children, and Class Members have sustained damages as a result of Brightline's breaches of the Contract, including breaches of the contracts entered into with Brightline through violations of the covenant of good faith and fair dealing.

COUNT IV

BREACH OF THIRD-PARTY BENEFICIARY CONTRACT (ON BEHALF OF PLAINTIFFS WATSON, ROSA, NDIFOR, AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

247. Plaintiffs restate and reallege all the allegations in paragraphs 1 through 176 as if fully set forth herein.

248. On information and belief, Brightline entered into contracts to provide services to its clients, including Plaintiff Watson's, Plaintiff Rosa's, and Plaintiff Ndifor's current and/or former employer(s), which services included data security practices, procedures, and protocols sufficient to safeguard the Private Information that was to be provided to it.

249. On information and belief, these contracts are virtually identical and were made expressly for the benefit of Plaintiffs and the Class, as it was their Private Information that Brightline agreed to receive and protect through its services. Thus, the benefit of collection, use, and protection of the Private Information belonging to Plaintiffs and the Class was the direct and primary objective of the contracting parties.

250. Brightline knew that if it were to breach these contracts with its clients, the clients' employees, including Plaintiffs and the Class Members, would be harmed.

251. Brightline breached its contracts with its clients—whose employees, including Plaintiffs and the Class Members—were affected by this Data Breach when it failed to use reasonable data security measures that could have prevented the Data Breach, and when it failed to timely notify Plaintiffs and Class Members regarding the breach.

252. As foreseen, Plaintiffs and the Class Members were harmed by Brightline's failure to use reasonable data security measures to store the Private Information Plaintiffs and Class Members provided to their respective employers and/or other entities, who in turn provided that Information to Brightline and the failure to timely notify Plaintiffs and Class Members, including

1 but not limited to, the continuous and substantial risk of harm through the loss of their Private
2 Information.

3 253. Accordingly, Plaintiffs and the Class Members are entitled to damages in an amount
4 to be determined at trial, including actual, consequential, and nominal damages, along with costs
5 and attorneys' fees incurred in this action.

6 **COUNT V**
7 **NEW JERSEY CONSUMER FRAUD ACT**
8 **N.J. S.A. §§ 56:8-1 ET SEQ.**
9 **(ON BEHALF OF PLAINTIFF MILNER AND THE NEW JERSEY SUBCLASS)**

10 254. Plaintiffs Milner restates and realleges all the allegations in paragraphs 1 through
11 176 as if fully set forth herein.

12 255. Brightline is a "person," as defined by N.J.S.A. § 56:8-1(d).

13 256. Brightline sells "merchandise," as defined by N.J.S.A. § 56:8-1(c) & (e).

14 257. The New Jersey Consumer Fraud Act ("CFA"), N.J.S.A. §§ 56:8-2 prohibits
15 unconscionable commercial practices, deception, fraud, false pretense, false promise,
16 misrepresentation, as well as the knowing concealment, suppression, or omission of any material
17 fact with the intent that others rely on the concealment, omission, or fact, in connection with the
18 sale or advertisement of any merchandise.

19 258. New Jersey CFA claims for unconscionable commercial practice need not allege
20 any fraudulent statement, representation, or omission by the defendant. *See Dewey v. Volkswagen*
21 *AG*, 558 F. Supp. 2d 505, 525 (D.N.J. 2008); *see also Cox v. Sears Roebuck & Co.*, 138 N.J. 2, 19
(1994).

22 259. "The standard of conduct that the term 'unconscionable' implies is lack of 'good
23 faith, honesty in fact and observance of fair dealing.'" *Cox*, 138 N.J. 2 at 18 (quoting *Kugler v.*
24 *Romain*, 58 N.J. 522, 544 (1971)). "In addition, '[i]ntent is not an essential element' for allegations
25 related to unconscionable commercial practices to succeed." *Fenwick v. Kay Am. Jeep, Inc.*, 72
26 N.J. 372, 379 (1977).

1 260. Brightline's handling and treatment of Plaintiff Milner's (and her child's) and New
2 Jersey Subclass Members' Private Information was unconscionable because:

- 3 a. Plaintiff and New Jersey Subclass Members had no choice but to provide
4 their Private Information to Brightline in order to use their Brightline
5 services;
- 6 b. To the extent that written contracts exist between Plaintiff and New Jersey
7 Subclass Members on the one hand and Brightline on the other hand, those
8 written contracts were written by Brightline and were not negotiable;
- 9 c. Once Plaintiff and New Jersey Subclass Members provided their Private
10 Information to Brightline, protection of that Private Information was solely
11 in Brightline's control. There is no way for Plaintiff or New Jersey Subclass
12 Members to take any reasonable steps on their own to protect the Private
13 Information in Brightline's hands; nor is there any way that Plaintiff and
14 New Jersey Subclass Members would have any knowledge that it would be
15 necessary for them to take steps on their own to protect their Private
16 Information;
- 17 d. Brightline knew, or should have known, that its data security was
18 inadequate and that it needed to take additional security measures to protect
19 Plaintiff's and New Jersey Subclass Members' Private Information, but
20 failed to do so, even though Brightline had a non-delegable duty to protect
21 Plaintiff's and New Jersey Subclass Members Private Information from
22 wrongdoers;
- 23 e. Once Brightline became aware of the Data Breach, it failed to timely notify
24 Plaintiff and New Jersey Subclass Members of the breach, thus depriving
25 them the opportunity to take measures to protect themselves from the effects
26 of Brightline's failure to protect their Private Information; and
27
28

f. Brightline's practices for handling and protecting Plaintiff's and New Jersey Subclass Members' Private Information was contrary to public policy in that Brightline failed to follow FTC and HIPAA guidelines with respect to the protection of Private Information – including PHI – and otherwise failed to follow industry standards for providing reasonable security and privacy measures to protect Plaintiff's and New Jersey Subclass Members' Private Information, which was a direct and proximate cause of the Data Breach.

261. Brightline's handling and treatment of Plaintiff's and New Jersey Subclass Members' Private Information was deceptive because Brightline:

- a. Misrepresented that it would protect the privacy and confidentiality of Plaintiff's and New Jersey Subclass Members' Private Information, including by implementing and maintaining reasonable security measures;
- b. Misrepresented that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTC Act, HIPAA, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*;
- c. Omitted, suppressed, and concealed the material fact that it did not properly secure Plaintiff's and New Jersey Subclass Members' Private Information; and
- d. Omitted, suppressed, and concealed the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff's and New Jersey Subclass Members' Private Information, including duties imposed by the FTCA, HIPAA, and the New Jersey Customer Security Breach Disclosure Act, N.J.S.A. §§ 56:8-163 *et seq.*

262. Brightline's representations and omissions were material because they were likely to deceive reasonable consumer-patients about the adequacy of Brightline's data security and ability to protect the confidentiality of patient Private Information.

263. Brightline intended to mislead Plaintiff and New Jersey Subclass Members and induce them to rely on its omissions of material fact.

264. Brightline acted intentionally, knowingly, and maliciously to violate New Jersey’s Consumer Fraud Act, and recklessly disregarded Plaintiff’s and New Jersey Subclass Members’ rights.

265. As a direct and proximate result of Brightline's unconscionable and deceptive practices, Plaintiff and New Jersey Subclass Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as alleged herein, including but not limited to fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; loss of value of their Private Information; overpayment for Brightline's services; loss of the value of access to their Private Information; and the value of identity protection services now made necessary by the Data Breach.

266. Plaintiff and New Jersey Subclass Members seek all monetary and non-monetary relief allowed by law, including injunctive relief, other equitable relief, actual damages, treble damages, restitution, and attorneys' fees, filing fees, and costs.

COUNT VI
VIOLATIONS OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS
PRACTICES ACT (“ICFA”)
(ON BEHALF OF PLAINTIFF JACKSON AND THE ILLINOIS SUBCLASS)

267. Plaintiffs Jackson restates and realleges all the allegations in paragraphs 1 through 176 as if fully set forth herein.

268. Plaintiff and Illinois Subclass Members are considered to be “persons” within the meaning of the statute, 815 Ill. Comp. Stat. § 505/1(c).

269. Defendant is also a “person” within the meaning of the same statute subsection.

1 270. Defendant engaged in deceptive acts or practices in the conduct of its business,
2 trade, and commerce or furnishing of services, in violation of ICFA, including:

- 3 a. Failing to implement and maintain reasonable security and privacy measures to
4 protect Plaintiff's and the Illinois Subclass Members' PII and PHI, which was a
5 proximate and direct cause of the Data Breach;
- 6 b. Failing to identify foreseeable security and privacy risks, remediate identified
7 security and privacy risks, and adequately improve security and privacy measures
8 following previous cybersecurity incidents, which was a direct and proximate cause
9 of the Data Breach;
- 10 c. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff's
11 and Illinois Subclass Members' PHI and PII, including by implementing and
12 maintaining reasonable security measures;
- 13 d. Failing to timely and adequately notify Plaintiff and Illinois Subclass Members of
14 the Data Breach;
- 15 e. Omitting, suppressing, and concealing the material fact that it did not reasonably or
16 adequately secure Plaintiff's and Illinois Subclass Members' PII and PHI; and
- 17 f. Omitting, suppressing, and concealing the material fact that it did not comply with
18 common law and statutory duties pertaining to the security and privacy of
19 Plaintiff's and Illinois Subclass Members' PII and PHI, including duties imposed
20 by the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, and COPPA, 15
21 U.S.C. §§ 6501-6505.

22 271. Defendant's representations and omissions were material because they were likely
23 to deceive reasonable consumers about the adequacy of Defendant's data security and ability to
24 protect the confidentiality of PII and PHI.

25 272. Defendant's representations and omissions were material because they were likely
26 to deceive reasonable consumer-patients.

273. Defendant acted intentionally and knowingly to violate ICFA, and recklessly disregarded Plaintiff's and Illinois Subclass Members' rights.

274. As a direct and proximate result of Defendant's deceptive and unlawful acts and practices, Plaintiff and the Illinois Subclass have suffered and/or are at a heightened and continual risk of suffering injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their PII and PHI.

275. Defendant's deceptive and unlawful acts and practices complained of herein affected the public interest and consumers at large.

276. The above deceptive and unlawful practices and acts by Defendant caused substantial injury to Plaintiff Jackson and Illinois Subclass Members that they could not reasonably avoid.

277. Plaintiff and the Illinois Subclass seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages, treble damages, injunctive relief, and attorney's fees and costs.

COUNT VII
VIOLATION OF THE TENNESSEE CONSUMER PROTECTION ACT,
TENN. CODE ANN. § 47-18-101, *ET SEQ.*
(ON BEHALF OF PLAINTIFFS AND THE TENNESSEE SUBCLASS)

278. Plaintiffs Castro restates and realleges all the allegations in paragraphs 1 through 176 as if fully set forth herein.

279. Tennessee's Identity Theft Deterrence Act ("ITDA"), under T.C.A § 47-18-2106, states that any violation of the ITDA "constitutes a violation of the Tennessee Consumer Protection Act[,] ("CPA"). The ITDA further states: "For the purpose of application of the [CPA], any violation of this part shall be construed to constitute an unfair or deceptive act or practice affecting trade or commerce and subject to the penalties and remedies as provided in that act, in addition to the penalties and remedies set forth in this part."

1 280. Defendant violated the ITDA because Defendant did not follow its provisions in
2 notifying Plaintiff and the Class about the Data Breach.

3 281. During the Data Breach, Defendant suffered a “breach of system security” as the
4 ITDA defines that term. Upon information and belief, Defendant maintained the Private
5 Information of Plaintiff and Tennessee Subclass Members in an unencrypted form, as defined in
6 Tenn. Code Ann. § 47-18-2107(a).

7 282. The ITDA defines “information holder” to include Defendant because Defendant
8 conducts business in Tennessee.

9 283. In Tenn. Code Ann. § 47-18-2107(a)(4), the ITDA defines “personal information”
10 to include Plaintiff’s and the Tennessee Subclass’s PII, including their names in combination with
11 the Social Security numbers, driver’s license numbers, or any “Account, credit card, or debit card
12 number, in combination with any required security code, access code, or password that would
13 permit access to an individual’s financial account[.]”

14 284. Following discovery of the Data Breach caused by unauthorized actors, the ITDA
15 required Defendant to notify all Tennessee residents whose “personal information was, or is
16 reasonably believed to have been, acquired by an unauthorized person. The disclosure must be
17 made no later than forty-five (45) days from the discovery or notification of the breach of system
18 security[.]” On information and belief, Defendant’s ongoing delay in notifying Plaintiffs and the
19 Class about the Data Breach was not “due to the legitimate needs of law enforcement” as defined
20 by ITDA.

21 285. Defendant failed to disclose the Data Breach to Plaintiffs and the Class within 45
22 days of discovering it, meaning it violated the CPA.

23 286. As a direct and proximate cause of Defendant’s ITDA and CPA violations, Plaintiff
24 and the Tennessee Subclass have suffered damages, including (i) the compromise, publication,
25 and/or theft of the Private Information; (ii) out-of-pocket expenses associated with the prevention,
26 detection, and recovery from identity theft and/or unauthorized use of their Private Information;
27 (iii) lost opportunity costs associated with effort expended and the loss of productivity addressing
28

and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (iv) the continued risk to their Private Information, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the Private Information in its continued possession, and (v) future costs in terms of time, effort, and money that will be expended as a result of the Data Breach for the remainder of the lives of Plaintiff and the Tennessee Subclass.

287. Plaintiff and the Tennessee Subclass are entitled to damages as well as injunctive relief, including, but not limited to, ordering Defendant to: (i) strengthen its data security systems, monitoring procedures, and data breach notification procedures; and (ii) immediately provide adequate credit monitoring to Plaintiff and the Tennessee Subclass.

COUNT VIII
VIOLATION OF CALIFORNIA CONSUMER RECORDS ACT, CAL. CIV. CODE §
1798.82, *ET SEQ.* ("CCRA")
(ON BEHALF OF PLAINTIFF NDIFOR AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE
CALIFORNIA SUBCLASS)

288. Plaintiffs Ndifor restates and realleges all the allegations in paragraphs 1 through 176 as if fully set forth herein.

289. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay. . . ."

290. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately

1 following discovery, if the personal information was, or is reasonably believed to have been,
2 acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b).

3 291. The CCRA specifies certain requirements when entities subject to its purview are
4 required to issue a security breach notification, including that such entities do not unreasonably
5 delay such notifications.

6 292. Brightline unreasonably delayed before sending notice of the breach to the Class.

7 293. As a result of Brightline’s violation of the CCRA, Plaintiff Ndifor and the Class
8 were deprived of prompt notice of the Data Breach and were thus prevented from taking
9 appropriate protective measures, such as securing identity theft protection or requesting a credit
10 freeze. These measures could have prevented some of the damages suffered by Plaintiff Ndifor
11 and Class Members because their stolen information would have had less value to identity thieves.

12 294. As a result of Brightline’s violation of the CCRA, Plaintiff Ndifor and the Class
13 suffered incrementally increased damages separate and distinct from those simply caused by the
14 Data Breach itself.

15 **COUNT IX**
16 **VIOLATION OF CALIFORNIA CONFIDENTIALITY OF MEDICAL INFORMATION**
17 **ACT, CAL. CIV. CODE § 56, *ET SEQ.* (“CMIA”)**
18 **(ON BEHALF OF PLAINTIFF NDIFOR AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE**
19 **CALIFORNIA SUBCLASS)**

20 295. Plaintiff Ndifor restates and realleges all the allegations in paragraphs 1 through
21 176 as if fully set forth herein.

22 296. Brightline is a “contractor,” as defined in Cal. Civ. Code § 56.05(d), a
23 “pharmaceutical company,” as defined in *id.* § 56.05(1), and “a provider of health care,” as defined
24 in Cal. Civ. Code § 56.06, and is therefore subject to the requirements of the CMIA, Cal. Civ.
25 Code §§ 56.10(a), (d) and (e), 56.36(b), 56.101(a) and (b).

26 297. Brightline is a person licensed under California under California’s Business and
27 Professions Code, Division 2. See Cal. Bus. Prof. Code § 4000, et seq. Brightline therefore
28 qualifies as a “provider of health care,” under the CMIA.

298. Plaintiff Ndifor and Class Members are “patients,” as defined in CMIA, Cal. Civ. Code § 56.05(k).

299. Brightline disclosed “medical information,” as defined in CMIA, Cal. Civ. Code § 56.05(j), to unauthorized persons without first obtaining consent, in violation of Cal. Civ. Code § 56.10(a). The disclosure of information to unauthorized individuals in the Data Breach resulted from the affirmative actions of Brightline’s employees, which allowed the hackers to see and obtain Plaintiff Ndifor’s and Class Members’ medical information.

300. Brightline’s negligence resulted in the release of PHI pertaining to Plaintiff Ndifor and the Class to unauthorized persons and the breach of the confidentiality of that information.

301. Brightline’s negligent failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiff’s and Class Members’ medical information in a manner that preserved the confidentiality of the information contained therein is a violation of Cal. Civ. Code §§ 56.06 and 56.101(a).

302. Brightline’s computer systems did not protect and preserve the integrity of electronic medical information in violation of Cal. Civ. Code § 56.101(b)(1)(A).

303. Plaintiff Ndifor and the Class were injured and have suffered damages, as described above, from Brightline’s illegal disclosure and negligent release of their medical information in violation of Cal. Civ. Code §§ 56.10 and 56.101, and therefore seek relief under Civ. Code §§ 56.35 and 56.36, including actual damages, nominal statutory damages of \$1,000, punitive damages of \$3,000, injunctive relief, and attorney fees, expenses and costs.

COUNT X
VIOLATION OF CALIFORNIA’S UNFAIR COMPETITION LAW, BUS. & PROF.
CODE § 17200, *ET SEQ.*
(ON BEHALF OF PLAINTIFF NDIFOR AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE
CALIFORNIA SUBCLASS)

304. Plaintiff Ndifor restates and realleges all the allegations in paragraphs 1 through 176 as if fully set forth herein.

305. The California Unfair Competition Law provides that:

1 “[U]nfair competition shall mean and include any unlawful, unfair
 2 or fraudulent business act or practice and unfair, deceptive, untrue
 3 or misleading advertising and any act prohibited by Chapter 1
 4 (commencing with Section 17500) of Part 3 of Division 7 of the
 5 Business and Professions Code.” (BUS. & PROF. CODE § 17200.)

6 306. Defendant stored the Private Information of Plaintiff Ndifor and the Class in its
 7 computer systems and knew or should have known it did not employ reasonable, industry standard
 8 and appropriate security measures that complied with applicable regulations and that would have
 9 kept Plaintiff’s and Class Members’ Private Information secure and prevented the loss or misuse
 10 of such.

11 307. Defendant failed to disclose to Plaintiff Ndifor and the Class that their Private
 12 Information was not secure. At no time were they on notice that their Private Information was not
 13 secure, which Defendant had a duty to disclose.

14 308. Had Defendant complied with these requirements, Plaintiff Ndifor and the Class
 15 would not have suffered the damages related to the Data Breach.

16 309. Defendant’s conduct was unlawful, in that it violated the policy set forth in (a)
 17 California’s Medical Information Act, requiring the safeguard of personal health information like
 18 the Private Information compromised as a result of the Data Breach, (b) HIPAA and the FTCA, as
 19 identified above, and (c) Defendant’s common law duty to safeguard PII and PHI.

20 310. Defendant’s conduct was also unfair, in that it violated a clear legislative policy in
 21 favor of protecting patients’ and Defendant’s clients’ employees’ Private Information from data
 22 breaches.

23 311. Defendant also engaged in unfair business practices under the “tethering test.” Its
 24 actions and omissions, as described above, violated fundamental public policies expressed by the
 25 California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1 (“The Legislature declares that . . . all
 26 individuals have a right of privacy in information pertaining to them . . . The increasing use of
 27 computers . . . has greatly magnified the potential risk to individual privacy that can occur from
 28

the maintenance of personal information.”); Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is a matter of statewide concern.”). Defendant’s acts and omissions thus amount to a violation of the law.

312. As a result of those unlawful and unfair business practices, Plaintiff Ndifor and the Class suffered an injury-in-fact and have lost money or property, be it tangible or intangible.

313. The injuries to Plaintiff and the Class greatly outweigh any alleged countervailing benefit to patients, consumers, or competition under all of the circumstances.

314. There were reasonably available alternatives to further Defendant’s legitimate business interests, other than the misconduct alleged in this complaint.

315. Therefore, Plaintiff Ndifor and the Class are entitled to equitable relief, including restitution of all monies paid to or received by Defendant; disgorgement of all profits accruing to Defendant because of its unfair and improper business practices; a permanent injunction enjoining Defendant’s unlawful and unfair business activities; and any other equitable relief the Court deems proper.

COUNT XI
UNJUST ENRICHMENT/QUASI CONTRACT
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

316. Plaintiffs restate and reallege all the allegations in paragraphs 1 through 176 as if fully set forth herein

317. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conferred upon, collected by, and maintained by Brightline, and that was ultimately stolen in the Data Breach.

318. Brightline benefitted by the conferral upon it of the Private Information pertaining to Plaintiffs and Class Members and by its ability to retain, use, sell, and profit from that information. Brightline understood that it so benefitted.

1 319. Brightline also understood and appreciated that Plaintiffs' and Class Members'
2 Private Information was in fact private and confidential, and its value depended upon Brightline
3 maintaining the privacy and confidentiality thereof.

4 320. But for Brightline's willingness and commitment to maintain its privacy and
5 confidentiality, Plaintiffs and Class Members would not have provided their Private Information
6 (and, in some cases, that of their children) to Brightline directly, or to their respective employers
7 to, in turn, provide that information to Brightline.

8 321. Because of its use of Plaintiffs' and Class Members' Private Information, Brightline
9 sold more services and products than it otherwise would have. Brightline was unjustly enriched by
10 profiting from the additional services and products it was able to market, sell, and create to the
11 detriment of Plaintiffs and Class Members.

12 322. Brightline also benefited through its unjust conduct by retaining money that it
13 should have used to provide reasonable and adequate data security to protect Plaintiffs' and Class
14 Members' Private Information.

15 323. Brightline further benefited through its unjust conduct in the form of the profits it
16 gained through the use of Plaintiffs' and Class Members' Private Information.

17 324. The benefits conferred upon, received, and enjoyed by Brightline were not
18 conferred officiously or gratuitously. Under the circumstances, it would be inequitable, unfair, and
19 unjust for Brightline to retain these wrongfully obtained benefits. Brightline's retention of
20 wrongfully obtained monies would also violate fundamental principles of justice, equity, and good
21 conscience.

22 325. As a result of Brightline's wrongful conduct as alleged in this Complaint (including,
23 among things, its failure to employ adequate data security measures; its continued maintenance
24 and use of the Private Information belonging to Plaintiffs and Class Members without having
25 adequate data security measures; and its other conduct facilitating the theft of that Private
26 Information), Brightline has been unjustly enriched at the expense of, and to the detriment of,
27 Plaintiffs and Class Members.
28

326. Brightline's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the compilation and use of Plaintiffs' and Class Members' sensitive Private Information, while at the same time failing to maintain that Information secure from intrusion and theft by hackers and identity thieves.

327. Brightline's defective data security and its unfair and deceptive conduct have, among other things, caused Plaintiffs and Class Members to unfairly incur substantial time and/or costs to mitigate and monitor the use of their Private Information and has caused the Plaintiffs and Class Members other damages as alleged herein.

328. Plaintiffs have no adequate remedy at law.

329. Brightline is therefore liable to Plaintiffs and Class Members for restitution or disgorgement in the amount of the benefit conferred on Brightline as a result of its wrongful conduct, including specifically: (a) the value to Brightline of the Private Information that was stolen in the Data Breach; (b) the profits Brightline received and is receiving from the use of that information; (c) the amounts that Brightline overcharged Plaintiffs and Class Members for use of Brightline's products and services; and (d) the amounts that Brightline should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' Private Information.

COUNT XII

BREACH OF CONFIDENCE

(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

330. Plaintiffs restate and reallege all the allegations in paragraphs 1 through 176 as if fully set forth herein

331. Plaintiffs and Class Members have an interest, both equitable and legal, in the Private Information about them that was conveyed to, collected by, and maintained by Defendant and ultimately accessed and acquired in the Data Breach.

332. As a provider of telehealth services, Defendant has a special relationship with its patients and with the employees of its clients, including Plaintiffs and Class Members (and their

1 children). Because of that special relationship, Defendant was provided with and stored Plaintiffs'
2 and Class Members' Private Information (and, in some cases, the Private Information of their
3 children) and had a duty to ensure that such was maintained in confidence.

4 333. Individuals whose Private Information was collected and maintained by Defendant
5 have a privacy interest in personal, medical and other matters, and Defendant had a duty not to
6 permit the disclosure of such matters concerning Plaintiffs and Class Members.

7 334. As a result of the parties' special relationship, Defendant had possession and
8 knowledge of highly sensitive and confidential PHI and PII belonging to Plaintiffs and Class
9 Members, information that was not generally known.

10 335. Plaintiffs and Class Members did not consent nor authorize Defendant to release or
11 disclose their Private Information to an unknown criminal actor.

12 336. Defendant breached its duty of confidence owed to Plaintiffs and Class Members
13 by, among other things: (a) mismanaging its system and failing to identify reasonably foreseeable
14 internal and external risks to the security, confidentiality, and integrity of patient and client
15 employee information that resulted in the unauthorized access and compromise of Plaintiffs' and
16 Class Members' Private Information; (b) mishandling its data security by failing to assess the
17 sufficiency of its safeguards in place to control these risks; (c) failing to evaluate and adjust its
18 information security program in light of the circumstances alleged herein; (d) failing to follow its
19 own privacy policies and practices published to its patients; and (e) making an unauthorized and
20 unjustified disclosure and release of Plaintiffs' and Class Members' Private Information to a
21 criminal third party.

22 337. But for Defendant's wrongful breach of its duty of confidence owed to Plaintiffs
23 and Class Members, their Private Information would not have been compromised.

24 338. As a direct and proximate result of Defendant's wrongful breach of its duty of
25 confidence, Plaintiffs and Class Members have suffered and will continue to suffer the injuries
26 alleged herein.

339. It would be inequitable for Defendant to retain the benefit of controlling and maintaining Plaintiffs' and Class Members' Private Information at the expense of Plaintiffs and Class Members.

340. Plaintiffs and Class Members are entitled to damages, including compensatory, punitive, and/or nominal damages, and/or disgorgement or restitution, in an amount to be proven at trial.

COUNT XIII
INJUNCTIVE/DECLARATORY RELIEF
(ON BEHALF OF PLAINTIFFS AND THE NATIONWIDE CLASS OR, ALTERNATIVELY, THE STATE SUBCLASSES)

341. Plaintiffs restate and reallege all the allegations in paragraphs 1 through 176 as if fully set forth herein.

342. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and to grant further necessary relief. Furthermore, the Court has broad authority to restrain acts that are tortious and violate the terms of the federal and state statutes described in this Complaint.

343. Defendant owes a duty of care to Plaintiffs and Class Members, which required them to adequately monitor and safeguard Plaintiffs' and Class Members' Private Information.

344. Defendant and its associates, vendors, and/or suppliers still possess the Private Information belonging to Plaintiffs and Class Members.

345. Plaintiffs allege that Defendant's data security measures remain inadequate. Furthermore, Plaintiffs continue to suffer injury as a result of the compromise of their Private Information and the risk remains that further compromises of their Private Information will occur in the future.

346. Under its authority pursuant to the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendant owes a legal duty to secure its patients' and clients' employees' Private Information under the common law, HIPAA, and the FTCA;

b. Defendant's existing data monitoring measures do not comply with its explicit or implicit contractual obligations and duties of care to provide reasonable data security procedures and practices that are appropriate to protect its patients' and client's employee's Private Information; and

c. Defendant continues to breach this legal duty by failing to employ reasonable measures to secure its patients' and clients' employees' Private Information.

347. This Court should also issue corresponding prospective injunctive relief requiring Defendant to employ adequate security protocols consistent with legal and industry standards to protect its patients' and client's employees' Private Information, including the following:

a. Order Defendant to provide lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members.

b. Order that, to comply with Defendant's explicit or implicit contractual obligations and duties of care, Defendant must implement and maintain reasonable security and monitoring measures, including, but not limited to:

i. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

ii. engaging third-party security auditors and internal personnel to run automated security monitoring;

iii. auditing, testing, and training its security personnel regarding any new or modified procedures;

iv. segmenting its user applications by, among other things, creating firewalls and access controls so that if one area is compromised, hackers cannot gain access to other portions of Defendant's systems;

v. conducting regular database scanning and security checks;

vi. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

vii. meaningfully educating its patients about the threats they face with regard to the security of their Private Information, as well as the steps Defendant's patients should take to protect themselves.

348. If an injunction is not issued, Plaintiffs will suffer irreparable injury and will lack an adequate legal remedy to prevent another data breach at Defendant. The risk of another such breach is real, immediate, and substantial. If another breach at Defendant occurs, Plaintiffs will not have an adequate remedy at law because many of the resulting injuries are not readily quantifiable.

349. The hardship to Plaintiffs if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Plaintiffs will likely be subjected to substantial, continued identity theft and other related damages if an injunction is not issued. On the other hand, the cost of Defendant's compliance with an injunction requiring reasonable prospective data security measures is relatively minimal, and Defendant has a pre-existing legal obligation to employ such measures.

350. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing a subsequent data breach at Defendant, thus preventing future injury to Plaintiffs and other patients and client employees whose Private Information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and the Class, seek the following relief:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Nationwide Class and State Subclasses as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiffs are proper representatives of the Nationwide Class and State Subclasses requested herein;

- b. Judgment in favor of Plaintiffs and Class Members awarding them appropriate monetary relief, including actual damages, statutory damages, equitable relief, restitution, disgorgement, and statutory costs;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;
- d. An order instructing Defendant to purchase or provide funds for lifetime credit monitoring and identity theft insurance to Plaintiffs and Class Members;
- e. An order requiring Defendant to pay the costs involved in notifying Class Members about the judgment and administering the claims process;
- f. A judgment in favor of Plaintiffs and Class Members awarding them prejudgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and
- g. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury on all triable issues.

DATED: October 2, 2023

Respectfully submitted,

/s/ Mason A. Barney

Mason A. Barney, Esq. (*Pro Hac Vice*)

Email: mbarney@sirillp.com

Kyle McLean, Esq. (SBN #330580)

Email: kmclean@sirillp.com

Tyler Bean, Esq. (*Pro Hac Vice*)

Email: tbean@sirillp.com

SIRI & GLIMSTAD LLP

700 S. Flower Street, Ste. 1000

Los Angeles, CA 90017

Telephone: 213-376-3739

Interim Class Counsel